bitdefender antivirus 2010

使用者手冊

BitDefender 病毒防護 2010
使用者手冊

出版 2009.09.18

法律聲明


bitdefender

內容目錄

使用者軟體授權合約

_如果您不同意這些條款和條件，請勿安裝此軟體。若在安裝前選擇了「我同意」、「確定」、「繼續」、「是」等選項，代表您完全了解及接受這份合約上的條款。

產品註冊。當接受此合約，您會同意使用"我的帳號"註冊您的產品，作為您產品使用與維護的條件(接收更新檔)。這個管控確保軟體只會在有效授權的電腦上使用，有效授權的使用者才能享有維護的服務。註冊需要一組有效的授權序號以及有效的電子郵件帳戶以使用續購優惠及其他法律條款。

對您來說，這個條款含概了 BitDefender 家用使用者的解決方案及服務，包含了相關的文件及任何應用程式的更新及升級，在您所購買的授權或任何相關的服務協定都定義在這份文件及任何這些條款的複本。

對於您與BITDEFENDER 公司來說，這份授權合約是份法律協議，在您使用BitDefender的軟體產品，它將涵概了電腦軟體、服務，可能包括了相關的媒體、列印的手冊及線上或電子式的文件，而這些都將被國際著作受權及國際商標法所保護。在安裝、複製及使用 BitDefender 時，您將同意這個協定上的條款。

如果您不同意這個合約上的條款，請不要安裝或使用 BitDefender。

BitDefender 授權。. 像智慧財產權法律及條款一樣，BitDefender 被著作權法律及國際受權條款所保護。BitDefender 是使用授權而非賣斷。

授權取得。BitDefender以此方式授權您個人並且有不可獨佔、有限的、不可轉移的使用BitDefender 授權。

軟體的使用。您可以按合約所訂的授權數量上安裝 BitDefender 軟體於許多電腦上。您也可以製作一份額外的複製光碟以備份為用途。

桌上型電腦使用者授權。這個 BitDefender 軟體授權可以安裝在個人電腦上，它並沒有提供網路服務。每個使用者可以安裝這個軟體在一台個人電腦，而且可以製作一份額外的複製當備份用途。主要使用者的數量依授權書上的使用者授權數量。

授權的期限。BitDefender 軟體的使用授權於購買日起至軟體到期日止。

使用期滿。當使用期滿時，產品會立即停止執行它的功能。

升級。如果BitDefender標示為升級版，你必須按照合約上規定正確地使用。如果是標示為升級替換或產品補助亦是你升級版的合格依據。你可以按使用合約上規定使用此升級版。 如果BitDefender升級只是整個產品的部分，你仍舊被授權使用單一產品，BitDefender或許可以被部分使用或傳遞但不可超過合約規定的使用數量。升級版的條款可能會取代或修改原先你與BitDenfender的原始條款。

版權。BitDefender之所有權利、標題、以及著作權 （包含任何影像、相片、企業標識、動畫、影片、聲音、音樂、文字及BitDefender內之applets ），與列印的材料、及 BitDefender 的任何複製版都屬 BITDEFENDER 公司所擁有。BitDefender 受到著作權法律及國際條款所保護。您必須對待 BitDefender 像其他有版權的媒體一樣。您不可以複製任何 BitDefender 附屬的文件。您必須在所有包含 BitDefender 的複製

媒體，附上所有的版權聲明。您不可再授權、租、售或分享 BitDefender 的授權。您不可利用反向工程、反編譯、拆解及建立衍生品、修改或解譯 BitDefender 原始程式碼。

有限保證。BITDEFENDER 保證從您收到 BitDefender 產品的 30 日內，可享有免費軟體媒體瑕疵更換的權利。BITDEFENDER 提供保證在收到瑕疵品後，可以選擇更換媒體或退還您購買 BitDefender 的金額。BITDEFENDER 不保證 BitDefender都沒有錯誤或錯誤都會被修正。BITDEFENDER 亦不保證 BitDefender 將符合您所有的需求。

除了合約書上明確的規定外，BitDefender不負責產品其他的明確或暗示性的保證包含改進、維護、支援或有形與無形的材料與服務。 BitDefender 明確地不對任何無限責任，適用於任何特定用途的保證、標題、資料與訊息內容準確性，以及過濾、中斷、清除其他公司軟體間諜程式、廣告軟體、郵件、 cookies 與文件擔負責任。 或是法令規章、交易條款、慣例與商業用途所導致的。

損害聲明。 任何人使用、測試、評估BitDefenderd可能存在影響BitDefender品質、性能上之風險，BitDefender 將不負任何責任。 BitDefender不對任何損害負責，包含無限的直接或間接使用上的損害，性能或傳送Bitdefender甚至是BitDefender已告知可能存在的損害。BitDefender所負責任將不超過您購買BitDefender的代價。以上聲明與有限責任，您自行決定是否接受使用，評估或測試BitDefender。

某些州不允許限制或排除對偶然損失或必然損失的責任，因此上述限制或排除可能不適用於您

BITDEFENDER的責任將不會超過您支付購買BITDEFENDER產品的價值金額。上述的免責條款和限制將會應用在不論是使用、評估或是測試BitDefender。

用戶重要通知. 本軟體不是容錯的也不是設計用在損壞時會自動啟動的作業環境。本軟體不適用於飛航作業，核能管控或通信系統、武器系統，直接或間接的生命支援監控系統或任何會導致死亡或身體及財產嚴重傷害之系統 。

電子通信同意書。. BitDefender會需要發送給您法律通知與其它關於軟體與維護授權服務的通信資訊，或是您提供給我們的資料的使用途徑。BitDefender將會透過產品內的聲明、或最初使用者註冊時使用的電子郵件帳號、或是公布在網站上發送通訊資料。接受此同意書，您將會同意只使用這些方式接受通信資訊，認可並表示您可以於網站存取通信資訊。

資料收集技術 – BitDefender告知您這樣的程式或產品會使用資料收集技術收集必要的技術資訊，以增進產品功能、提供相關服務、採用並防止未授權或非法產品使用、或是惡意程是造成的傷害。您接受BitDefender在產品使用這樣的技術來提供服務並防止惡意程式影響您的電腦。

您同意並接受BitDefender提供的更新或是額外的程式會自動下載到您的電腦。

藉由接受此合約，您同意上傳可執行的檔案讓BitDefender伺服器進行掃描。相同地，由於建構與使用程式的緣故，您會必須提供BitDefender個人資料。BitDefender告知您它會基於隱私權條款的章規使用您的資料。

資料收集。訪問網站的用戶和收購產品和服務以及使用的工具或內容通過網站意味著處理個人資料。遵守法例規管處理個人數據和信息社會服務和電子商務是極其重要的BitDefender。有時，為了獲取產品，服務的內容或工具，您會在某些情況下，需要提供某些個人資料。 BitDefender保證這些數據會絕對保密，並按照法例規管的保護個人數據和信息社會服務和電子商務。

BitDefender符合適用的數據保護立法，並採取了行政和技術的必要步驟，以保證它收集的個人資料安全。

您聲明的所有數據，您會提供真實、準確、並承諾在通知BitDefender任何變化表示的數據。您有權反對任何處理他或她的數據，是沒有必要的執行協議，並把它用於任何維護合同關係之外的用途。

倘若您提供第三方的細節，BitDefender不會追究責任的原則，遵守信息和同意，因此，應保證您有事先通知並得到同意的所有者的數據，關於這些數據的溝通。

BitDefender和其分支與合作夥伴將僅通過電子郵件或其他電子手段發送營銷信息給這些已提供他們明確表示同意收到信函BitDefender產品或服務或簡報的用戶。

BitDefender的隱私權條款，保證您的權利透過電子郵件：juridic@bitdefender.com 訪問、糾正、消除和反對的數據處理通知BitDefender。

一般條款。本合約受羅馬尼亞及國際版權之管轄。如有任何違反條款其裁決管轄為羅馬尼亞法院。

本合約的任一條款如有失效，此一失效的條款將不影響本合約的其他條款。

BitDefender與其logos是屬BitDefender之商標，在本產品用到所有其他商標與相關的材料屬其他個別公司所有。

如您違反任何條款，本合約將立即終止且不予事先通知。而您也得不到BitDefender或其經銷商任何賠償，且合約條款有關使用上之保密與限制依然有效。

BitDefender可在任何時間修政條款，而修正後的條款將自動地在推出的相關版本的軟體使用且不影響其他條款的有效性。

在各種翻譯語文如有爭議或不一致性時，以BitDefender的英文版條款為基準。

聯絡 BITDEFENDER, 於 24, Preciziei Boulevard, West Gate Building H2, ground floor, Sector 6, Bucharest, Romania, 或請電: 40-21-206.34.70 or Fax: 40-21-264.17.99, E-mail 信箱: office@bitdefender.com.

序言

這份手冊提供給選擇BitDefender 病毒防護 2010做為他們個人電腦上的安全解決方案。在這本書上的資訊不只是適合提供給電腦操作者使用，也適合任何一個可以在 Windows 環境下的使用者使用。

這本書將會為您解釋BitDefender 病毒防護 2010，並帶領您操作安裝、設置的過程。您可以了解如何使用BitDefender 病毒防護 2010，如何更新、測試並自訂您想要的內容。您將學習到如何使用BitDefender。

我們希望您有一個愉快且有用的演講。

1. 本書的用法說明

1.1. 印刷上的常規

為了易於閱讀，此書使用了幾種文字的樣式。它們的外觀及意思描述在以下的表格裡面。

外觀	描述
sample syntax	語法樣本一起列印monospaced特性.
http://www.bitdefender.com	這個 URL 連結正指到其他外部的位置，http 或 ftp 伺服器。
sales@bitdefender.com	在文字中插入聯絡的電子郵件位址資訊。
"序言" (p. xiii)	這是一個內部的連結，連結到這份手冊的其他位置。
filename	檔案及目錄使用monospaced 字型列印。
option	所有產品選項使用strong字元來列印。
sample code listing	程式的列表使用monospaced字元列印。

1.2. 警告

警告是以文字、圖表來標示，針對目前的段落，提醒您額外的資訊。



註

註解只是很短的意見。儘管您可以略過它，註解可以提供有價值的資訊，像是特定的功能或連結到一些相關的主題。



重要

這個要求您的注意並且建議不要跳過它。通常它提供非絕對重要但卻是有意義的資訊。



警告

這是極重要的資訊，您必須重視它。如果您依指示去做，將不會有壞的事發生。您應該仔細閱讀並了解它，因為它描述了極危險的事。

2. 本書的架構

本書包含幾個部份包含了幾個主題。 此外，有一個詞彙表讓您清楚一些技術的詞彙。

安裝與移除. 依循步驟指示安裝BitDefender到個人電腦。您會被指引如何進行安裝程序。最後，也會讓您了解如何移除BitDefender。

開始使用. 包含讓您能夠開始使用BitDefender的所有資訊。將會介紹您有關使用者介面以及修復事件，設置基本的設定並註冊產品。

一般檢視模式. 顯示BitDefender的一般模式使用者介面。

進階檢視模式. 詳細的顯示為BitDefender進階模式使用者介面。 您會被指導如何設定及使用所有BitDefender模組，使您能更有效地保護您的電腦對抗所有惡意程式的威脅 (病毒、間諜程式、後門程式及其他威脅)。

整合Windows 和第三方軟體. 讓您知道如何透過Windows右鍵選單使用BitDefender的選項，以及使用與第三方軟體整合的BitDefender工具列。

如何. 讓您可以快速運行最常使用的BitDefender任務。

問題排除並取得協助. 如果有一些未預期的情況發生，從何找尋及詢問，以取得協助。

BitDefender 救援光碟. BitDefender 救援光碟描述。它協助了解及使用這個可開機光碟所提供的功能。

詞彙表. 詞彙表能夠解釋您在本書上發現的一些技術專有名詞及罕見的項目說明。

3. 意見回饋

我們邀請您協助我們改進這份手冊。我們將盡全力測試及確認所有的資訊。當您發現在這份手冊中任何瑕疵，或者您認為該如何改進以提供給您最好的檔案，請寫下來告訴我們。

透過電子郵件寄到documentation@bitdefender.com讓我們知道。



重要

請用英文寫下您的所有檔案相關的電子郵件，我們可以更有效率地處理它們。

安裝與移除

1. 系統需求

您只能在以下的作業系統中安裝BitDefender 病毒防護2010：

- Windows XP (32/64 位元)與Service Pack 2 或更高
- Windows Vista (32/64位元)或Windows Vista Service Pack 1或更新版本
- Windows 7 (32/64位元)

在安裝之前，請確定您的電腦符合最低的硬體以及軟體要求。



註
要找出您所使用的作業系統版本以及硬體資訊，在桌面上的 我的電腦 點擊右鍵，然後選取 內容。

1.1. 系統需求

- 450 MB 可用的硬碟空間
- 800 MHz 的處理器
- RAM ：
  - 使用Windows XP：512 MB
  - 1 GB 於 Windows Vista 與 Windows 7
- Internet Explorer 6.0
- .NET Framework 1.1 (可以在套件中安裝)

1.2. 建議的系統需求

- 600 MB 可用的硬碟空間
- Intel CORE Duo (1.66 GHz) 或相容處理器
- RAM ：
  - 1 GB 於 Windows Vista 與 Windows 7
  - 1.5 GB 於 Windows Vista
- Internet Explorer 7 (或更高版本)
- .NET Framework 1.1 (可以在套件中安裝)

1.3. 支援的軟體

網路釣魚防護只能在這些地方使用：

- Internet Explorer 6.0 (或更高版本)
- Mozilla Firefox 2.5
- Yahoo 即時通 8.5
- Windows Live Messenger 8

即時通訊加密只能在這些地方使用：

- Yahoo 即時通 8.5

- Windows Live Messenger 8

2. 準備安裝

在安裝BitDefender 病毒防護 2010之前，請完成下列準備以確保安裝順利：

- 請確定要安裝BitDefender的系統已達到最低系統需求。 若電腦沒有達到最低系統，可能會導致BitDefender無法安裝、正常運作，或是系統不穩定。 要了解更多資訊，請參閱“系統需求” (p. 2)。
- 使用系統管理員帳號登入電腦。
- 移除電腦上其他的防毒軟體。 在同一電腦上安裝了個防毒軟體會導致產品運作與系統不穩定等問題。 進行安裝前，Windows Defender會被停用。

3. 安裝BitDefender

您可以使用BitDefender 安裝CD或是從我們的官方網站下載安裝檔進行安裝。 您在此http://www.bitdefender.com/site/Downloads/下載BitDefender 產品安裝檔。

- 要使用CD安裝，請將CD放入光碟機。請稍待片刻，歡迎畫面將會出現即可以開始安裝。

  若CD沒有進入安裝畫面，請進入CD的路徑Products\Antivirus\install\en\並點擊兩下runsetup.exe。

- 您可以下載並使用BitDefender安裝檔並執行安裝程式。

安裝程式會先確認電腦的安裝狀態。 安裝驗證後，設定精靈將會出現。 下列圖像表示安裝設定精靈。



安裝步驟

請依照以下步驟來安裝BitDefender病毒防護 2010:

1. 點擊 下一步。 您可以點擊取消安鈕中止安裝。

   如果您的電腦已安裝其他的病毒防護產品，BitDefender 病毒防護 2010 會發出警告。 點擊移除 以移除所有已安裝的元件。 如果您不要移除已刪除的產品，點擊下一步繼續進行安裝。

   警告
   在安裝BitDefender之前，強烈建議您先移除其他的病毒防護軟體。同時使用兩個或以上的病毒防護軟體，會影響電腦系統的運作。

2. 請詳讀授權合約並點擊我同意。

   重要
   如果您不同意這些條款，則點擊 取消。這個安裝程序將被中止，您將離開這個設定。

3. 選擇要安裝的類型。
   - 典型 - 使用預設的設定進行安裝。 若您要選擇此項目，請跳到步驟六。
   - 自訂 - 您可自行設置安裝設定。 此選項讓您可以便更安裝路徑。

4. BitDefender 病毒防護 2010的預設安裝路徑為：C:\Program Files\BitDefender\BitDefender 2010。 如果您要變更安裝路徑，點擊瀏覽並選取您要安裝 BitDefender 病毒防護 2009 的目錄。。

   點擊 下一步。

5. 選取安裝程序的相關選項。 其中有些選項為預設：
   - 開啟閱讀我檔案 — 在軟體安裝結束後，開啟讀我檔案。
   - 在桌面放一個捷徑 — 在軟體安裝結束後，在您的桌面上放一個 BitDefender 防毒標準版 2010 的捷徑。
   - 安裝完成後退出CD - 在安裝完成後把CD退出；當你選擇用CD安裝時會出現此選項。
   - 停用DNS快取 - 停用DNS快取。 DNS用戶端服務可能被惡意程式利用來在網路散佈有害資訊。
   - 關閉Windows Defender - 把Windows Defender關閉；此選項只適用於Windows Vista。

   點擊 安裝 開始進行軟體的安裝。 如果您尚未安裝，BitDefender 會首先安裝.NET Framework 1.1。

6. 等到安裝完成後，點擊完成。 您的系統可能被要求重新啟動，以便安裝精靈完成你的安裝程序。 我們建議您盡快重新啟動。



重要

在完成安裝並重新啟動之後，將會出現註冊精靈 以及 設置精靈。 完成這些精靈的程序以註冊並設置您的BitDefender 病毒防護 2010，並建立一個BitDefender帳號。

如果您接受了預設的安裝路徑，您可以在Program Files看到一個新的資料夾BitDefender並包含子資料夾 BitDefender 2010。

3.1. 註冊精靈

完成安裝後第一次啟動電腦時，註冊精靈將會出現。 精靈將會幫助您註冊BitDefender並設置您的BitDefender 帳號。

您必須建立一個帳號以收到BitDefender更新檔案。 擁有BitDefender帳號，您可以享有免費的技術支援及特別的續購優惠。 如果您遺失了BitDefender授權序號，您可以透過http://myaccount.bitdefender.com並登入您的帳號以重新取得您的授權序號。



註

如果您不想使用這個精靈，點擊 取消。 您可以在任何時候執行註冊精靈，在使用者介面下方點擊註冊。

3.1.1. 步驟 1 — 註冊 BitDefender 病毒防護2010

BitDefender Antivirus 2010

註冊精靈

BitDefender 註冊

我想要評估BitDefender

我想用授權序號註冊 BitDefender

輸入授權序號：

授權序號: 輸入授權序號 立刻註冊

沒有授權序號？立即購買!

要了解 BitDefender 使用介面的各個選項，請將滑鼠移到該選項，即可顯示相對應的文字解釋。

取消 上一步 下一步

註冊

BitDefender 病毒防護 2010 有30天試用期。 要繼續評估產品，點選我要評估BitDefender並點擊下一步。

註冊BitDefender 病毒防護 2010：

1. 選取 我想要使用序號註冊產品。

2. 在編輯欄位中輸入授權序號。



註

您可以在這些地方找到授權序號：

- 光碟標籤。
- 產品註冊卡。
- 線上購買的電子郵件。

如果您沒有BitDefender的授權序號，您可以連線至BitDefender 線上商店購買授權序號。

3. 點擊立即註冊。

4. 點擊 下一步。

若在您的系統偵測到有效的序號，您可以點擊下一步繼續使用序號。

3.1.2. 步驟 2 — 建立一個 BitDefender 帳號

建立帳號

如果您不想建立 BitDefender 帳號，選取 稍候註冊並點擊完成。 否則，根據您目前的狀況選擇：

- "我沒有BitDefender 帳號" (p. 9)
- "我已經擁有BitDefender 帳號。" (p. 10)



重要

您必須在安裝BitDefender15天內建立一個帳號(試用期將會被延長至30天)。 否則，BitDefender將不再繼續更新。

我沒有BitDefender 帳號

要順利建立BitDefender帳號，請依循下列步驟：

1. 選取建立一個新帳號。
2. 在對應的欄位輸入必要的資訊。 您在這裡所提供的資料將會被保密。
   - E-mail address — 輸入您的電子郵件信箱。
   - 密碼 — 為您的BitDefender帳號輸入一組密碼。 密碼長度必須要有6-16個字元。
   - 重複鍵入密碼 — 重新輸入先前的密碼。



註
一旦帳號被啟用，您可以http://myaccount.bitdefender.com輸入您的電子郵件位址與密碼登入帳號。

3. 您可以在BitDefender帳號所登記的電子郵件信箱，收到特別的續購優惠的相關訊息。 從選單選取一個選項：
   - 傳送所有訊息
   - 只傳送給我產品相關的訊息
   - 不要傳送任何訊息
4. 點擊建立。
5. 點擊完成 以關閉精靈。
6. 啟用您的帳號。. 在能夠您的帳號前，您必須先啟動。 檢查您的EMAIL並且依循信中的BitDefender registration service指示完成程序。

我已經擁有BitDefender 帳號。

BitDefender 將會自動發現您先前電腦上登記的 BitDefender 帳號。 在這個狀況，請提供您的帳號密碼並點擊登入。 點擊完成 以關閉精靈。

若您已經擁有一個啟動的帳號，但BitDefender沒有偵測到，請依循這些步驟註冊：

1. 點選登入(先前註冊的帳號)。
2. 在對應的欄位輸入電子郵件位址與密碼。



註
如果您忘記您的密碼，點擊 忘記您的密碼？ 並依循指示操作。

3. 您可以在BitDefender帳號所登記的電子郵件信箱，收到特別的續購優惠的相關訊息。 從選單選取一個選項：
   - 傳送所有訊息
   - 只傳送給我產品相關的訊息
   - 不要傳送任何訊息
4. 點擊登入。
5. 點擊完成 以關閉精靈。

3.2. 設置精靈

在完成註冊精靈後，設置精靈將會出現。 這個精靈會協助您進行重要的設置並選擇適合您的使用介面。在精靈的最後，您將會更新惡意程式碼並掃描系統的檔案，

精靈包含數個簡單的步驟。步驟的數量取決於您的選擇。 在此列出全部的步驟，但您的選擇會影響步驟的數量。

完成這個精靈並非強制的；然而，我們建議您如此做以節省時間並且確定您的系統在 BitDefender 病毒防護 2010 安裝前是安全的。 如果您不想使用這個精靈，點擊 取消。 BitDefender 在您開啟使用者介面時，將會提醒您需要設置的元件。

3.2.1. 步驟1 - 選擇設定檔



使用設定檔

點擊按鈕點選適合本電腦的設定檔。

選項	描述
典型	點擊這裡，若這台電腦主要用於上網和多媒體活動。
遊戲	點擊這裡，這台電腦主要用來執行電腦遊戲。
自定	點擊這裡若您要進行完整的功能設置。

您可以從產品使用介面重設設定檔。

3.2.2. 步驟2 - 描述電腦



電腦描述

點擊適用您電腦的選項：

- 您的電腦在家庭網路中。. 檢及此選項若您要從遠端管控其他電腦的BitDefender產品。 精靈將會出現協助您設置家庭網路管理模組。
- 本電腦是筆記型電腦. 點擊此選項若您要筆電模式預設是啟動的。 在筆電模式中，排程的掃描任務將不會進行。

點擊 下一步以繼續。

3.2.3. 步驟3 - 選擇使用介面



使用者介面檢視模式

點擊按鈕選擇最適合您的使用介面。 根據您的電腦使用技巧以及對於BitDefender的經驗，您可以在三種模式中檢視使用者介面。

模式	描述
新手模式	適合電腦的初學者以及那些想使用BitDefender 保護電腦但不想受到額外干擾的人。這個模式容易使用，只需要最少量的使用者互動。 您只需要事件被BitDefender找出來時去修復它即可。有個簡單的精靈將會幫助您修復事件。 此外，您可以執行常用任務，像是更新產品與病毒碼或是執行病毒掃描。
一般模式	針對有普通電腦使用技巧的使用者，這個模式是新手模式的延伸。 您可以分別修復事件，並選取要監控的事件。 此外，您可以遠端管理在您住家中已安裝BitDefender產品的電腦。
進階模式	適合更具有技術的使用者，這個模式讓您能夠完整的設置BitDefender的每個功能。 您也可以使用所有的任務來保護您的電腦。

3.2.4. 步驟4 - 設置BitDefender 網路



註
此步驟只會在您選擇設置家庭網路時才會出現。



BitDefender網路設置

BitDefender 讓您能夠在家中的電腦間建立一個虛擬網路，並管理網路中安裝的BitDefender 。

如果您要這台電腦成為BitDefender家庭網路的一部分，請依照以下步驟：

1. 點選啟動家庭網路。
2. 在編輯欄位中輸入相同的管理密碼。 密碼能夠讓管理者從其他電腦管理這台電腦上的BitDefender 。

點擊 下一步以繼續。

3.2.5. 步驟5 - 選擇要執行的任務



選擇任務

為您的系統安全，設定BitDefender以執行重要的防護任務。 有以下選項可選：

- 更新BitDefender並執行快速系統掃描 - 在下個步驟將會執行BitDefender檔案更新作業以提供最完善的防護。 當更新完成時，BitDefender將會掃描Windows與Program Files資料夾的檔案以確保系統安全。 這些包含作業系統檔案與安裝程式的資料夾最容易受到感染。。
- 在每天2 AM執行系統掃描 - 設定BitDefender在每天2 AM執行系統掃描。 要編更執行的時間，請點擊選單並選擇適合的時間。 若到了排程的時間但是電腦沒有啟動，任務會在您下次開機時執行。



註

若要變更排程的時間，請依循下列步驟：

1. 開啟BitDefender 並將使用者介面切換至進階模式。
2. 從左側選單點擊 病毒防護。
3. 點擊 病毒掃描標籤。
4. 滑鼠右鍵點選系統掃描任務並點選排程。 將會開啟一個新的視窗。
5. 變更頻率與開始的時間。
6. 點擊確定 去儲存變更。

建議在進到下一個步驟之前您啟動這些選項以確保您的系統安全。 點擊 下一步以繼續。

若您清除第一個方塊，則在精靈結束時不會執行任務。 點擊完成 以關閉精靈。

3.2.6. 步驟 6 — 完成



任務狀態

等待BitDefender運行更新。 當更新完成時，將會開始快速系統掃描。 掃描將在背景隱匿執行。 您可看見掃描程序圖示出現在系統列。 您可以點擊此圖示開啟掃描視窗並檢視掃描程序。

點擊完成 以關閉精靈。 您不需要等待掃描結束。



註

掃描任務將會需要一段時間。 當掃描結束時，開啟掃描視窗並檢視掃描結果。 若掃瞄過程有偵測到病毒，您應該立刻開啟BitDefender 並執行一次完整的系統掃描。

4. 升級

若您使用BitDefender 病毒防護 2010beta、2009、2008，您可以升級成BitDefender 病毒防護 2010版。

升級有兩種方式可以進行：

- 直接安裝BitDefender Antivirus 2010 若您是直接從2009版升級，隔離區的資料會被自動匯入。
- 移除舊的版本，重新開機並安裝新的版本，請參閱“安裝BitDefender” (p. 5)。產品設定將不會被儲存。 若其他方式失敗，請使用此方法。

5. 修復或移除BitDefender

若您想要修復或移除BitDefender 病毒防護 2010，請依照Windows 開始程式集的路徑：開始 → 程式集 → BitDefender 2010 → 修復或移除。

您將被要求點擊 下一步去確認您的選擇。一個可讓您選擇的新視窗將會出現：

- 修復 — 重新安裝先前設定時的所有程式元件。

  如果您選擇修復BitDefender，將會出現一個新的視窗。 點擊修復以開始進行修復程序。

  重新啟動電腦，然後點擊安裝以重新安裝 BitDefender 病毒防護 2010。

  當安裝程序完成，將會出現一個新的視窗。 點擊 完成。

- 移除 — 移除所有已安裝的元件。



註
我們建議選擇移除當需要完全重新安裝元件。

如果您選擇了移除BitDefender，將會出現一個新視窗。



重要
只有在Windows Vista! 當移除BitDefender時，您的系統不再免於惡意軟體的威脅，例如：病毒、間諜程式。 如果您希望Windows的系統防護在移除BitDefender後開啟，請選擇對應的核取方塊。

按下移除以開始從您的系統中移除BitDefender 病毒防護 2010。

當移除過程完成後，將會出現一個新的視窗。 點擊 完成。



註
移除程序完成後，我們建議您刪除 BitDefender 目錄位於 Program Files裡。

開始使用

6. 總覽

只要您安裝BitDefender ，您的電腦就會被保護。 若您還沒有完成設置精靈，您必須盡快開啟BitDefender主畫面並修復事件。 您必須要設置特定的BitDefender元件或預防的動作以保護您的電腦資料。 若有需要，您可以設定BitDefender不要提示您特定的事件。

若您尚未註冊產品 (包含建立帳號)，在產品試用到期前，請不要忘記註冊。 您必須在安裝BitDefender15天內建立一個帳號(試用期將會被延長至30天)。 否則，BitDefender將不再繼續更新。 要瞭解更多註冊程序資訊，請參考 "註冊與我的帳號" (p. 41)。

6.1. 開啟BitDefender

要進入BitDefender 2010的主介面，請依循下面路徑使用Windows 開始程式集 開始 → 程式集 → BitDefender 2010 → BitDefender 病毒防護 2010 或更快的方法，在系統工具列上按兩下 BitDefender小圖示。

6.2. 使用者介面檢視模式

BitDefender 病毒防護2010能滿足不同使用者的需求。因此我們設計圖示型的使用者介面，讓每個使用者都能順利的使用。

根據您的電腦使用技巧以及對於BitDefender的經驗，您可以在三種模式中檢視使用者介面。

模式	描述
新手模式	適合電腦的初學者以及那些想使用BitDefender 保護電腦但不想受到額外干擾的人。這個模式容易使用，只需要最少量的使用者互動。 您只需要事件被BitDefender找出來時去修復它即可。有個簡單的精靈將會幫助您修復事件。 此外，您可以執行常用任務，像是更新產品與病毒碼或是執行病毒掃描。
一般模式	針對有普通電腦使用技巧的使用者，這個模式是新手模式的延伸。 您可以分別修復事件，並選取要監控的事件。 此外，您可以遠端管理在您住家中已安裝BitDefender產品的電腦。
進階模式	適合更具有技術的使用者，這個模式讓您能夠完整的設置BitDefender的每個功能。 您也可以使用所有的任務來保護您的電腦。

使用者介面模式是在設置精靈中選擇。 這個精靈會在註冊精靈之後，在您安裝後第一次啟動電腦時出現。 如果您取消了設置精靈，使用者介面將會預設在一般模式。

要變更操作模式，請依循這些步驟：

1. 開啟BitDefender。
2. 點擊設定 鈕，在視窗的右上角。
3. 在使用者介面設定分類，點擊按鈕上的箭頭 以選取您想要的模式。
4. 點擊確定 以儲存並套用變更。

6.2.1. 初學者檢視模式

如果您是個電腦的初學者，使用新手模式可能會最適合您。 這個模式容易使用，只需要您最少量的互動。



初學者檢視模式

此畫面分為四個主要索引：

- 安全狀態 提示可能影響電腦安全的事件並協助您修復。 點擊修復所有事件，將有一個精靈幫助您簡單的移除影響您電腦安全的威脅 要了解更多資訊，請參考 “修復事件” (p. 32)。
- 保護您的電腦 您可以在此找到需要的任務以保護您的電腦安全。 您可使用的任務項目取決於您所選的使用設定檔。
  - 立刻掃描按鈕可以開始一個標準的系統掃描。 病毒防護掃描精靈將會出現並帶領您完成掃描程序。 要了解更多資訊，請參考 “病毒掃描精靈” (p. 46)。

- 立刻更新按鈕協助您升級BitDefender的病毒碼與產品檔案。 您可以在新開啟的視窗檢視更新狀況。 若偵測到更新，它會自動下載並安裝到您的電腦。
- 當選擇典型設定檔，系統弱點檢查會協助您修復系統上的弱點。 要了解更多資訊，請參閱"系統弱點檢查精靈" (p. 56)。
- 當選擇遊戲玩家設定檔，開啟/關閉遊戲模式讓您可以啟動/停用 遊戲模式。 遊戲模式能夠暫時地變更防護設定，將系統運行的影響減至最低。

- 維護您的電腦 您可以在此找到需要的任務以保護您的電腦安全。
  - 深度系統掃描啟動強大的掃描任務掃描您的系統。
  - 我的文件掃描在My Documents與Desktop掃描可疑的檔案。
  - 自動登入掃描掃描登入系統時執行的項目。
- 設定檔表示目前所選的使用介面設定。 使用設定檔顯示這台電腦主要的活動。根據不同的使用設定檔，使用者介面將會有不同的組織方式以迎合您的使用需求。

  如果您想切換或變更使用設定檔，點及設定檔並依照設置精靈操作。

在視窗的右上角，您可以看到 設定 鈕。打開視窗您可以變更使用者介面模式，以及啟動或停用 BitDefender的主要設定。 要了解更多資訊，請參考"設置一般設定" (p. 35)。

在視窗的右下角您可以看到幾個有用的連結。

連結	描述
購買/續購	開啟您可以購買BitDefender 2010產品的畫面。
註冊	提供您輸入新的授權序號，或檢視目前的授權序號及註冊狀態。
說明 & 支援	進入說明文件，讓您了解如何使用BitDefender。

6.2.2. 一般檢視模式

針對一般的電腦使用者，一般模式提供了使用所有模組的基本操作，您必須持續追蹤警示以及修復不想要的事件。



一般檢視模式

一般模式視窗包含五個標籤，下列的表格簡單的解釋每個標籤。 要了解更多資訊，請參閱"一般檢視模式" (p. 63)。

標籤	描述
狀態顯示表	顯示系統的安全狀態並可以設置設定檔。
病毒防護	顯示病毒防護模組的狀態，幫助您保持BitDefender 在更新狀態以保護您的電腦不受病毒侵入。
反網路釣魚	顯示反網路釣魚的狀態。
系統弱點	顯示弱點檢查模組的狀態，幫助您保持電腦中重要軟體的更新。您可在此修復可能影響電腦安全的系統弱點。
網路	顯示BitDefender 家庭網路結構。 您可在此設置並管理您的BitDefender家庭網路設定。 如此，您從單一電腦可以管理您家中的網路。

在視窗的右上角，您可以看到 設定 鈕。打開視窗您可以變更使用者介面模式，以及啟動或停用 BitDefender的主要設定。 要了解更多資訊，請參考"設置一般設定" (p. 35)。

在視窗的右下角您可以看到幾個有用的連結。

連結	描述
購買/續購	開啟您可以購買BitDefender 2010產品的畫面。
註冊	提供您輸入新的授權序號，或檢視目前的授權序號及註冊狀態。
支援	提供您連結至BitDefender支援小組。
說明	進入說明文件，讓您了解如何使用BitDefender。
檢視日誌	提供您查看BitDefender在您的系統進行的所有任務的詳細歷史。

6.2.3. 進階檢視模式

您可以在進階模式進入每個特定的BitDefender元件。 您可在此進行BitDefender的細節設定。



註
進階模式適合擁有高於平均電腦使用技巧的使用者，並了解您電腦所暴露的威脅類型，以及安全程式如何運作。

進階檢視模式

在視窗的左端有一個選單，包含所有的安全模組。 每個模組包含一個或數個標籤，以設置對應的安全設定或安全任務。 下列的表格簡單描述了各個模組。 要了解更多資訊，請參閱“進階檢視模式” （p. 82）。

模組	描述
一般	提供您存取一般設定，或檢視狀態顯示表和詳細的系統資訊。
病毒防護	提供您詳細設置您的病毒防禦及掃描操作，設定例外及設置隔離區模組。
隱私權管控	在您使用網路時預防資料竊取並保護您的隱私。
弱點檢查	提供您保持電腦中重要軟體的更新。
加密	提供您加密Yahoo即時通和Windows Live (MSN) Messenger的傳訊。
遊戲/筆電模式	當您使用電池運作電腦時，提供您延緩BitDefender排定的任務，在您玩遊戲時忽略警示及彈出式視窗。
網路	提供您設置與管理您家庭網路中的電腦。
更新	提供您獲得最近更新的資訊，更新產品與設置更新程序。
註冊	提供您註冊BitDefender病毒防護2010、變更授權序號、或是建立一個BitDefender帳號。

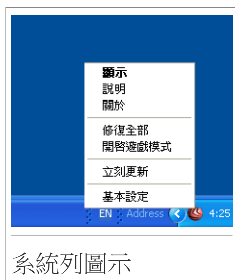
在視窗的右上角，您可以看到 設定 鈕。打開視窗您可以變更使用者介面模式，以及啟動或停用 BitDefender的主要設定。 要了解更多資訊，請參考“設置一般設定” (p. 35)。

在視窗的右下角您可以看到幾個有用的連結。

連結	描述
購買/續購	開啟您可以購買BitDefender 2010產品的畫面。
註冊	提供您輸入新的授權序號，或檢視目前的授權序號及註冊狀態。
支援	提供您連結至BitDefender支援小組。
說明	進入說明文件，讓您了解如何使用BitDefender。
檢視日誌	提供您查看BitDefender在您的系統進行的所有任務的詳細歷史。

6.3. 系統列圖示

要更快速的管理整個產品，您可以使用BitDefender 的圖示 於系統列中。 如果您連按二下這個圖示，BitDefender會被開啟。您也可以按下滑鼠右鍵，在出現的右鍵選單進行 BitDefender 的快速管理。



系統列圖示

- 顯示 - 開啟主要介面。
- 說明 - 開啟說明檔案，您可以進一步了解如何使用BitDefender 2010。
- 關於 - 開啟一個視窗，在此您可以得到更多關於BitDefender的資訊，並尋求相關協助。
- 修復所有事件 - 幫助您消除目前的安全弱點。 若這個選項無法使用，則沒有事件需要修復。 要了解更多資訊，請參考“修復事件” (p. 32)。
- 開啟/關閉遊戲模式 - 啟動 / 停用遊戲模式。
- 立即更新 - 立刻執行更新。 您可以在新開啟的視窗檢視更新狀況。
- 基本設定 - 開啟一個視窗以變更使用者介面模式或啟動/停用主要的產品設定。 要了解更多資訊，請參考“設置一般設定” (p. 35)。

BitDefender的系統列圖示透過如下的不同符號，在事件影響您的電腦時提醒您，或是產品的運行狀態：

有驚嘆號的紅色圈圈： 影響您系統安全的重大事件，這需要立刻的關注並儘快解決。

有驚嘆號的黃色三角形： 非重大的事件影響您的電腦安全，您應該於有空閒時間時檢查並修復這些事件。

代碼G: 產品在遊戲模式運作。

如果BitDefender沒有在運作，圖示將會是灰色的。 這通常發生於授權序號到期，或是BitDefender 沒有回應時。

6.4. 掃瞄活動列

這個 掃描活動列 是您的系統上掃描活動的圖形。 這個小視窗只預設會出現於進階模式。

灰色線條(檔案區)顯示每秒掃描的檔案數量，從0到50的範圍。



註
當即時保護停用時，掃瞄活動列會在檔案區顯示一個紅色叉叉來提醒您。



掃瞄活動列

6.4.1. 掃描檔案與資料夾

您可以使用掃描活動列掃描檔案與資料夾。 拖放您想要掃描的檔案或資料夾到下方顯示的 掃描活動列。



拖曳檔案



放開檔案

病毒防護掃描精靈將會出現並帶領您完成掃描程序。 要了解更多資訊，請參考 "病毒掃描精靈" (p. 46)。

掃描選項. 掃描選項是為了最佳的掃描效果而設置。 若偵測到受感染的檔案，BitDefender 將會嘗試解毒。 若消毒失敗，病毒掃描精靈將會允許您採取其他動作。 這是標準的掃描設定，您不能加以變更。

6.4.2. 停用/恢復掃描活動列

當您不想再看到這個即時的圖形顯示，請按下滑鼠右鍵，並選擇隱藏。 要恢復掃描活動列，請依循下列步驟：

1. 開啟BitDefender。
2. 點擊設定 鈕，在視窗的右上角。
3. 在一般設定分類，選取對應掃描工具列的核取方塊。
4. 點擊確定 以儲存並套用變更。

6.5. BitDefender 手動掃瞄

BitDefender手動掃描任務讓您可以指定要掃描的資料夾或是硬碟。 這個功能是設計用來在Windows的安全模式執行。 若系統被感染病毒，您可以嘗試在Windows安全模式之下使用手動掃描功能，偵測病毒並嘗試解毒。

如果您想執行BitDefender手動掃瞄，請依照Windows 開始程式集的路徑： 開始 → 程式集 → BitDefender 2010 → BitDefender 手動掃描 以下視窗將會顯示：



BitDefender 手動掃瞄

點擊 加入資料夾，選擇要掃描的位置並點擊 確定。 若要掃描多個資料夾，請重覆此動作。

您所選擇的位置將會出現在掃描目標欄位。 如果您要變更路徑，只要點擊旁邊的 移除鈕。 點擊移除全部路徑鈕以移除所有加入清單的位置。

當您選好位置，點擊繼續。 病毒防護掃描精靈將會出現並帶領您完成掃描程序。 要了解更多資訊，請參考 "病毒掃描精靈" (p. 46)。

掃描選項. 掃描選項是為了最佳的掃描效果而設置。 若偵測到受感染的檔案，BitDefender 將會嘗試解毒。 若消毒失敗，病毒掃描精靈將會允許您採取其他動作。 這是標準的掃描設定，您不能加以變更。

什麼是安全模式?
安全模式是專為Windows發生問題時所使用的開機模式， 在安全模式下，Windows只會啟動最基本的元件與驅動程式。大部分的程式都無法在安全模式啟動，所以可以在安全模式下將病毒順利刪除。
在電腦開機時，按下F8鍵，即可進入安全模式選單。若您要在安全模式下能夠存取網路，請選擇安全模式 含網路功能選項。



註

要了解更多資訊，請到開始功能表，點選說明與支援。 您也能在網路上找到有用的資訊。

6.6. 遊戲模式與筆電模式

某些電腦的動作，例如遊戲或簡報，需要增加系統的反應與效能，且不能被打擾。 當您的筆電正在使用電池十，最好將那些非必要性的操作，延後至連接電源時再進行。

為了適應這些特殊的情況，BitDefender 病毒防護 2010 包括了兩個特殊的操作模式：

- 遊戲模式
- 筆電模式

6.6.1. 遊戲模式

遊戲模式能夠暫時地變更防護設定，將系統運行的影響減至最低。 當您啟動遊戲模式，下列設定將會被套用：

- 使處理程序時間和記憶體消耗降到最低
- 延緩自動更新和自動掃描
- 消除所有警示和彈出式視窗
- 只掃描最重要的檔案

當遊戲模式啟動時，您可以看見英文字母G顯示在 BitDefender圖示上。

執行遊戲模式

預設BitDefender 會在您所設定的遊戲或全螢幕應用程式啟動時自動開啟遊戲模式。BitDefender 將會在偵測到您關閉遊戲或結束全螢幕程式後自動回到普通操作模式。

可以選擇下列其中一種方式手動啟動遊戲模式：

- 在系統工具列按下滑鼠右鍵點擊 BitDefender 圖示，並選擇 啟動遊戲模式。
- 同時按下 Ctrl+Shift+Alt+G 鍵(預設熱鍵)。



重要
請記得在您遊戲結束時關閉遊戲模式。只要重複執行開啟的方式，即可關閉。

變更遊戲模式熱鍵

如您想更改快速鍵，請按照以下步驟：

1. 開啟BitDefender 並將使用者介面切換至進階模式。
2. 於左側選單點擊 遊戲/筆電模式。
3. 點擊遊戲模式標籤。
4. 點擊進階設定鈕。
5. 在使用熱鍵選項，設定您要的熱鍵：
   - 您可以按下：Ctrl鍵(Ctrl)、Shift鍵(Shift)、Alt鍵(Alt)以選擇使用它們當做熱鍵。
   - 在編輯欄鍵入字母以對應熱鍵。

   舉例而言，如果您想要用Ctrl+Alt+D當作熱鍵，您必須按下Ctrl與Alt並且輸入D。



註
取消選取使用熱鍵就可以停用熱鍵。

6. 點擊確定 去儲存變更。

6.6.2. 筆電模式

筆電模式特別為筆電的使用者設計，將可以在您使用電池為電源時，對筆電的電力消費影響達到最低。 在筆電模式中，排程的掃描任務將不會進行。

BitDefender 偵測到您的筆電使用電池為電源時，將自動進入筆電模式。 而BitDefender 在偵測到您不再使用電池為電源時，將自動離開筆電模式。

要使用筆電模式，您必須在設置精靈 設定您使用的是筆電。 如果您沒有在精靈中選取適當的選項，您可以依照下列步驟稍後啟動筆電模式：

1. 開啟BitDefender。
2. 點擊設定 鈕，在視窗的右上角。
3. 在一般設定分類，選取對應筆電模式偵測的核取方塊。
4. 點擊確定 以儲存並套用變更。

6.7. 自動裝置偵測

BitDefender 自動偵測連接可移除式的儲存裝置，並在存取檔案之前提供您掃描。 建議您以此保護您的電腦免於病毒或其他惡意程式的威脅。

偵測到的裝置分成以下幾個類別：

- CD/DVD

- USB儲存裝置，例如隨身碟或外接硬碟
- 已定位的(遠端)網路磁碟

當這些裝置被偵測到，會顯示一個警示視窗。



裝置偵測警示

要掃描儲存裝置，點擊是。．病毒防護掃描精靈將會出現並帶領您完成掃描程序。 要了解更多資訊，請參考 “病毒掃描精靈” (p. 46)。

如果您不想掃描裝置，點擊 否。在這個情況下，您可以找到以下有用的選項：

- 不要在問我有關這種裝置 - BitDefender 將不會在提供您自動掃描的選項。
- 停用自動裝置偵測 - 在您連接裝置至電腦時，將不會被提醒掃描。

如果您意外的停用了自動裝置偵測，而想要啟動它，或是您想要設置設定，依照下列步驟：

1. 開啟BitDefender 並將使用者介面切換至進階模式。
2. 到 病毒防護>病毒掃描。
3. 在掃描任務列表中，選取 裝置偵測掃描 任務。
4. 右鍵點擊任務並選取開啟。 將會開啟一個新的視窗。
5. 在總覽 標籤，設置掃描選項。 要了解更多資訊，請參考 “調整掃描設定” (p. 103)。
6. 在 偵測 標籤，選取您想要偵測的儲存裝置類型。
7. 點擊確定 以儲存並套用變更。

7. 修復事件

BitDefender 使用事件追蹤系統以偵測可能影響您電腦安全的事件。預設只監控少數被認為非常重要的事件，您也可以自己選取要監控的事件類型。

這是擱置的事件如何被提醒的方法：

- 一個特殊的符號將會顯示在BitDefender系統列圖示上以代表有擱置的事件。

  有驚嘆號的紅色圈圈： 影響您系統安全的重大事件，這需要立刻的關注並儘快解決。
  有驚嘆號的黃色三角形： 非重大的事件影響您的電腦安全，您應該於有空閒時間時檢查並修復這些事件。

  如果您將游標移到圖示上，將會出現一個彈出式視窗提醒您有擱置的事件。

- 當您開啟BitDefender時，安全狀態區域將會告訴您影響您電腦安全的事件數量。
  - 在一般模式中，安全狀態顯示於狀態顯示表標籤中。
  - 在進階模式中，到一般>狀態顯示表以檢查安全狀態。

7.1. 修復所有事件精靈

修復事件最簡單的方法就是依照修復所有事件精靈的步驟。 這個精靈協助您移除可能影響您電腦的任何威脅。 要開啟精靈，依照下列操作：

- 右鍵點擊系統列中的BitDefender圖示並選取t 修復所有事件。
- 開啟BitDefender。 根據使用者介面模式，如以下進行：
  - 在新手模式中，點擊修復所有事件。
  - 在一般模式中，到狀態顯示表標籤並點擊修復所有事件。
  - 在進階模式中，到一般>狀態顯示表標籤並點擊修復所有事件。



修復所有事件精靈

精靈顯示您電腦存在的安全防護弱點列表。

所有現有的事件都被選取要修復。如果您有不想修復的事件，請選取對應的核取方塊。如果您這樣做，狀態將會變更為跳過。



註
如果您不想被通知某些事件，您必須在追蹤系統一一設置。

要修復選取的事件，點擊開始。某些事件將會立即修復，而其他的將會有精靈來幫助您修復。

這個精靈幫助您修復的事件可以分成以下幾個主要分類：

- 停用安全設定.　透過啟動對應的安全設定，有些事件將會立即修復。
- 您應該執行的安全防護任務.　例如掃描您的電腦。建議您至少一個禮拜掃描一次您的電腦，大部份的情況下BitDefender 將會自動完成。然而如果您變更了掃描排程，或是排程沒有完成，您將會被提醒有這個事件存在。

  修復這些事件時，將會出現一個精靈幫助您完成任務。
- 系統弱點.　BitDefender會自動檢查您的系統弱點並提醒您進行修復。 系統弱點包含下列：
  - Windows使用者帳號的危險密碼。
  - 您電腦上的過期產品。

- ☐錯過的Windows更新。
- ☐Windows自動更新已停用

當要修復這些事件時，弱點檢查掃描精靈將會開啟，這個精靈幫助您修復偵測到的系統弱點。 要了解更多資訊，請參閱"系統弱點檢查精靈" (p. 56)。

7.2. 設置事件追蹤

事件追蹤系統監控並提醒您可能影響您電腦安全的事件。額外的事件監控決定於您在設置精靈的選擇。 除了預設監控的事件，有幾個事件您也可以設置被通知。

透過選取您想要被通知的事件，您可以自行設置最適合您的事件追蹤系。您可以在一般或進階模式中進行此操作。

- 在一般模式中，追蹤系統可以在分散的位置中設置。 依循下列步驟:
  1. 到病毒防護，反網路釣魚或系統弱點標籤。
  2. 點擊設置狀態追蹤.
  3. 選取對應的核取方塊以監控項目。

  要了解更多資訊，請參閱"一般檢視模式" (p. 63)。
- 在進階模式中，追蹤系統可以由中央管控。 依循下列步驟:
  1. 到一般>狀態顯示表.
  2. 點擊設置狀態追蹤.
  3. 選取對應的核取方塊以監控項目。

  要了解更多資訊，請參考"狀態顯示表" (p. 83)。

8. 設置一般設定

您可以設置主要產品設定(包括變更使用者檢視介面)從基本設定視窗，要打開視窗，依照下列任何一個方法：

- 開啟BitDefender並點擊畫面右上角的設定連結。
- 右鍵點擊系統列中的BitDefender圖示 並選取 基本設定。



註

要詳細設置產品設定，使用進階模式。 要了解更多資訊，請參閱“進階檢視模式” (p. 82)。



基本設定

設定分為三個部分：

- 使用者介面設定
- 安全設定
- 一般設定

要套用並儲存您所作的設置變更，點擊確定。不儲存變更並關閉視窗，點擊取消。

8.1. 使用者介面設定

在這個區域，您可以切換使用者介面模式，並重新設定使用設定檔。

切換使用者介面檢視模式。. 像在“使用者介面檢視模式” (p. 20)頁面中解釋的一樣，有三種使用者介面的顯示模式。每個模式分別設計給不同的使用者，主要以電腦的使用技能作為區分。 使用者介面適合所有類型的使用者，從電腦的新手到十分有技巧的使用者。

第一個按鈕顯示目前的使用者介面模式。 在使用者介面設定分類，點擊按鈕上的箭頭 以選取您想要的模式。

模式	描述
新手模式	適合電腦的初學者以及那些想使用BitDefender 保護電腦但不想受到額外干擾的人。這個模式容易使用，只需要最少量的使用者互動。 您只需要事件被BitDefender找出來時去修復它即可。有個簡單的精靈將會幫助您修復事件。 此外，您可以執行常用任務，像是更新產品與病毒碼或是執行病毒掃描。
一般模式	針對有普通電腦使用技巧的使用者，這個模式是新手模式的延伸。 您可以分別修復事件，並選取要監控的事件。 此外，您可以遠端管理在您住家中已安裝BitDefender產品的電腦。
進階模式	適合更具有技術的使用者，這個模式讓您能夠完整的設置BitDefender的每個功能。 您也可以使用所有的任務來保護您的電腦。

重新設定使用設定檔。. 使用設定檔顯示這台電腦主要的活動。根據不同的使用設定檔，使用者介面將會有不同的組織方式以迎合您的使用需求。

要重新設置使用設定檔，點擊重新設定使用設定檔並依照設置精靈操作。

8.2. 安全設定

在這個區域您可以啟動或停用包含您電腦安全的產品設定。 設定的目前狀態以以下的圖示中其中一個表示：

- 打勾的綠色圈圈： 設定已啟動。
- 有驚嘆號的紅色圈圈： 設定已停動。

要啟動/停用一個設定，請選取/清除對應的啟動核取方塊。



警告

當即時防護停用時，請謹慎使用電腦。 停用這些功能可能會危害您的電腦安全。 若您必須要停用，請盡快將它們恢復。

所有設定的清單和描述提供於下列的表格中：

設定	描述
病毒防護	即時檔案防護確保您存取與執行應用程式時所有的檔案都會經過掃描。
自動更新	動更新確保BitDefender產品及特徵碼檔案會定期下載並安裝更新。
系統弱點檢查	自動系統弱點檢查確保您電腦中的重要軟體的更新。
反網路釣魚	即時反網路釣魚防護能夠提醒您正在瀏覽的網頁可能有陷阱。
身分管控	身分管控確保您不會傳送包含個人資料的訊息到網路上，它將會阻擋即時通訊、電子郵件或網際網路上的個人資料。
即時通訊加密	即時通訊加密確保您透過Yahoo!即時通和MSN的訊息安全，但是您的聯絡人也必須使用相容的BitDefender和即時通訊軟體版本。

某些設定狀態會被BitDefender 事件追蹤系統。 如果您停用了監控設定，BitDefender 將會顯示為一個需要修復的事件。

如果您不想要已停用的設定被顯示為事件，您必須設置追蹤系統。您可以在一般模式或進階模式使用此操作。

- 在一般模式中，追蹤系統根據設定分類，可以在分散的位置中設置。 要了解更多資訊，請參閱"一般檢視模式" （p. 63）。
- 在進階模式中，追蹤系統可以由中央管控。 依循下列步驟:
  1. 到一般>狀態顯示表.
  2. 點擊設置狀態追蹤.
  3. 清除對應的核取方塊以取消監控項目。

  要了解更多資訊，請參考"狀態顯示表" （p. 83）。

8.3. 一般設定

在這個區域，您可以啟動或停用影響產品行為和使用者經驗的設定。 要啟動/停用一個設定，請選取/清除對應的啟動核取方塊。

所有設定的清單和描述提供於下列的表格中：

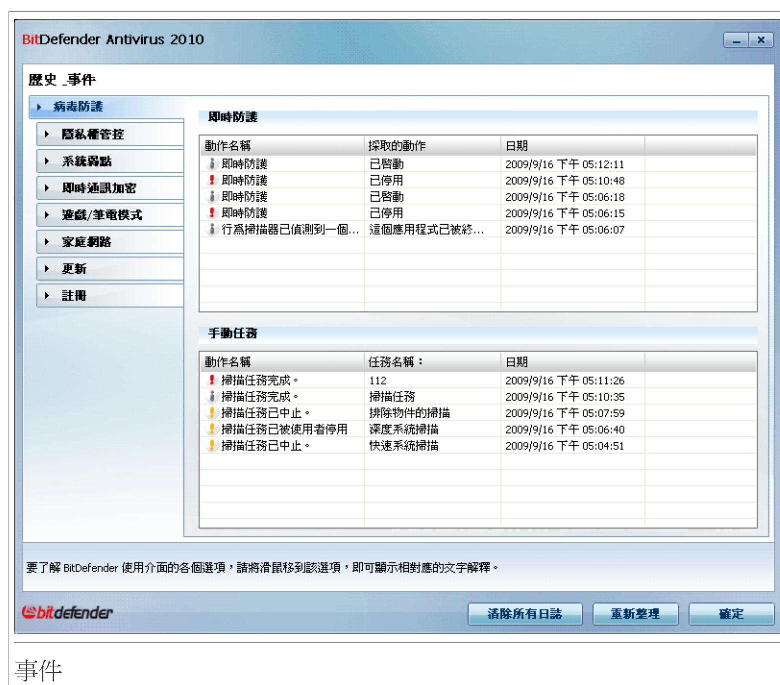
設定	描述
遊戲模式	遊戲模式可以暫時調整防護設定以減少對遊戲運行的影響。
筆電模式偵測	筆電模式可以暫時調整防護設定以減少對筆電電池的消耗。
設定密碼	確保BitDefender設定將經過密碼保護。 啟動這個選項，您將會被提醒設置設定密碼。 在兩個欄位中輸入想要的密碼並點擊確定 以設置密碼。
BitDefender新聞	啟動這個選項，您將收到重要的BitDefender公司訊息、產品更新訊息或新的安全威脅訊息。
產品提示警示	啟動這個選項，您將收到資訊警示。
掃描活動列	掃描活動列會顯示目前BitDefender的掃描活動。 要了解更多資訊，請參考“掃瞄活動列” (p. 26)。
傳送病毒報告	啟動這個選項，將傳送病毒掃描報告至BitDefender實驗室進行分析。這個報告將不會含有隱私資料，例如您的名字或IP位置，也不會被用來進行商業活動。
病毒疫情偵測	啟動這個選項，潛在病毒疫情報告將傳送至BitDefender實驗室進行分析。這個報告將不會含有隱私資料，例如您的名字或IP位置，也不會被用來進行商業活動。

9. 歷史與事件

在BitDefender主視窗下方的 檢事日誌選項將可以開啟另一個視窗BitDefender歷史&事件。這個視窗提供您檢視與安全性相關的事件。 例如您可以輕易地檢查最近是否有成功的更新，有沒有惡意程式在您的電腦裡頭被發現等等。



註
這個連結只有在一般或進階模式才能使用。



事件

為了協助您過濾BitDefender歷史紀錄&事件，視窗左側將提供以下目錄：

- 病毒防護
- 隱私權管控
- 系統弱點
- 即時通訊加密
- 遊戲/筆電模式
- 家庭網路
- 更新
- 註冊。

●網際網路日誌

每一個目錄都有一個可用的事件清單，每個清單包含下列資訊：簡短的敘述、BitDefender所執行的動作、發生的時間日期。如果您想了解更多只需要在事件上點擊兩下即可。

點擊 清除日誌 以清除舊的日誌。點擊 重新整理 以顯示最新的日誌。

10. 註冊與我的帳號

BitDefender 病毒防護 2010 有30天試用期。 在試用期間內，您可測試完整的產品功能以了解是否符合您的需求。 請注意，除非您建立了BitDefender 帳號，否則15天過後，產品會停止更新。 建立帳號是註冊程序最重要的步驟之一。

在試用日期結束前，您必須註冊產品以持續保護您的系統。 註冊有兩個程序:

1. 產品啟動 (註冊BitDefender帳號). 　您必須建立帳號才能接收產品更新並使用免費支援。 　若您已經有一個帳號，請直接使用該帳號註冊。 　BitDefender將會通知您啟用帳號，並協助您修復問題。



重要

您必須在安裝BitDefender15天內建立一個帳號(試用期將會被延長至30天)。 否則，BitDefender將不再繼續更新。

2. 用授權序號註冊. 　授權序號指定您可以使用產品的時間長度。 當授權序號到期，BitDefender 停止它的功能並保護您的電腦。 在試用到期前，您必須用授權序號註冊產品。 在授權快到期時，您應該購買一組序號或是續購您的授權。

10.1. 註冊BitDefender 病毒防護 2010

如果您想要以授權序號註冊產品或是變更目前的授權序號，點擊立即註冊連結於BitDefender 視窗最下方。 註冊視窗將會出現。

BitDefender Antivirus 2010

註冊精靈

BitDefender 註冊

目前的授權序號狀態：

類型： 可用的, 試用

到期於: 30 天

輸入授權序號：

授權序號: 輸入授權序號 　立刻註冊

沒有授權序號？立即購買!

要了解 BitDefender 使用介面的各個選項，請將滑鼠移到該選項，即可顯示相對應的文字解釋。

取消 　上一步 　下一步

註冊

您可以檢視BitDefender 註冊狀態，現在使用的授權序號，以及授權序號將在幾天內到期。

註冊BitDefender 病毒防護 2010：

1. 在編輯欄位中輸入授權序號。



註
您可以在這些地方找到授權序號：

- 光碟標籤。
- 產品註冊卡。
- 線上購買的電子郵件。

如果您沒有BitDefender的授權序號，您可以連線至BitDefender 線上商店購買授權序號。

2. 點擊立即註冊。
3. 點擊 完成。

10.2. 啟動BitDefender

要啟動BitDefender，您必須建立或登入一個BitDefender帳號。 如果您在初始註冊精靈沒有註冊BitDefender帳號的話，您可以依照下列步驟：

- 在新手模式中，點擊修復所有事件。 這個精靈將會幫助您修復所有擱置的事件，包括啟動產品。
- 在一般模式，到安全防護標籤並點擊對應有關產品啟動事件的修復按鈕。
- 在進階模式中，到註冊 並點擊啟動產品鈕。

帳號註冊視窗將會開啟。 您可以在此建立或登入BitDefender 帳號以啟動您的產品。

建立帳號

如果您不想建立 BitDefender 帳號，選取 稍候註冊並點擊完成。 否則，根據您目前的狀況選擇：

- “我沒有BitDefender 帳號” (p. 43)
- “我已經擁有BitDefender 帳號。” (p. 44)



重要

您必須在安裝BitDefender15天內建立一個帳號(試用期將會被延長至30天)。 否則，BitDefender將不再繼續更新。

我沒有BitDefender 帳號

要順利建立BitDefender帳號，請依循下列步驟：

1. 選取建立一個新帳號。
2. 在對應的欄位輸入必要的資訊。 您在這裡所提供的資料將會被保密。
   - E-mail address — 輸入您的電子郵件信箱。
   - 密碼 — 為您的BitDefender帳號輸入一組密碼。 密碼長度必須要有6-16個字元。
   - 重複鍵入密碼 — 重新輸入先前的密碼。



註
一旦帳號被啟用，您可以http://myaccount.bitdefender.com輸入您的電子郵件位址與密碼登入帳號。

3. 您可以在BitDefender帳號所登記的電子郵件信箱，收到特別的續購優惠的相關訊息。 從選單選取一個選項：
   ●傳送所有訊息
   ●只傳送給我產品相關的訊息
   ●不要傳送任何訊息
4. 點擊建立。
5. 點擊完成 以關閉精靈。
6. 啟用您的帳號。. 在能夠您的帳號前，您必須先啟動。 檢查您的EMAIL並且依循信中的BitDefender registration service指示完成程序。

我已經擁有BitDefender 帳號。

BitDefender 將會自動發現您先前電腦上登記的 BitDefender 帳號。 在這個狀況，請提供您的帳號密碼並點擊登入。 點擊完成 以關閉精靈。

若您已經擁有一個啟動的帳號，但BitDefender沒有偵測到，請依循這些步驟註冊：

1. 點選登入(先前註冊的帳號)。
2. 在對應的欄位輸入電子郵件位址與密碼。



註
如果您忘記您的密碼，點擊 忘記您的密碼？ 並依循指示操作。

3. 您可以在BitDefender帳號所登記的電子郵件信箱，收到特別的續購優惠的相關訊息。 從選單選取一個選項：
   ●傳送所有訊息
   ●只傳送給我產品相關的訊息
   ●不要傳送任何訊息
4. 點擊登入。
5. 點擊完成 以關閉精靈。

10.3. 購買授權序號

若試用期即將結束，您必須購買序號並註冊產品。 開啟BitDefender並點擊畫面下方的購買/續購連結。 這個連結會轉到一個購買的網頁。

10.4. 續購您的授權

若您試BitDefender的顧客，在續購時，您可以獲得產品折扣。 在授權期限內，您可以免費獲得的產品升級更新。

若您目前的序號即將要到期，您必須續購您的授權。 開啟BitDefender並點擊畫面下方的購買/續購連結。 這個連結會開啟一個可以續購您的授權的網頁。

11. 精靈

為了讓BitDefender更容易使用，數個精靈協助您完成安全任務並設置複雜的產品設定。 這個章節解釋在您修復事件和執行任務時會出現的精靈。 其他設置的精靈分別在“進階檢視模式” (p. 82)部份解釋。

11.1. 病毒掃描精靈

當您使用任何掃描任務時I(用BitDefender掃描)，BitDefender病毒掃描精靈將會出現。Select 依照三步驟指引執行掃描任務。



註

若掃描精靈沒有出現，則此任務可能被設為在背景作業。 您可以在系統工具列看見掃描程序圖示。 您可以點擊此圖示開啟掃描視窗並檢視掃描程序。

11.1.1. 步驟 1/3 — 進行掃描

BitDefender 將會開始掃描選擇的項目。



掃瞄中

您能見到掃描狀態和統計 (掃描速度, 使用時間, 掃描 / 受傳染的 / 可疑的 / 隱藏的物件和其他的數目)。

等待BitDefender 完成掃描。



註
掃描程序將依它的複雜程度而需花費一些時間。

密碼保護的封存檔. BitDefender 在掃描過程偵測到一個密碼保護的封存檔，預設的動作是詢問密碼，您會被詢問要提供密碼。 受密碼保護的檔案無法被掃描。 有以下選項可選：

- 我要輸入此物鍵的密碼. 若您要BitDefender掃描封存檔，點選此選項並鍵入密碼。若您不知道密碼，選擇其他選項。
- 我不想輸入此物件的密碼 (跳過此物件). 選擇此選項跳過掃描封存檔。
- 我不想輸入任何物件的密碼 (跳過所有密碼保護的物件). 選擇此項目若您要不被詢問任何密碼保護的項目。 BitDefender 將不會掃描它們但會紀錄在掃描日誌檔案。

點擊 確定以繼續掃描。

停止或暫停掃描. 您可以點擊停止，完全停止掃描程序，而您將會直接被引導到最後的步驟。 您可以點擊暫停，暫時停止掃描程序。點擊 回復以繼續掃描任務。

11.1.2. 步驟 2/3 — 選擇動作。

當掃描程序完成，一個新的視窗會出現，您可以在該視窗檢視掃描結果。



動作

您可以檢視可能影響您的系統的事件數量。

被感染的物件會依照感染它們的惡意程式分組做表示。 點擊對應的威脅，您便可以得到更多關於被感染物件的資訊。

您可以針對不同的威脅類型的分組採取全體行動，也可以逐項地進行處理。

下列的選項會出現在選單中：

動作	描述
沒有採取動作	不對偵測到的檔案採取任何行動。 掃描完成後，您可以開啟掃描記錄檢視掃描結果。
消毒檔案	從受感染的檔案中移除惡意程式碼。
刪除檔案	刪除所有被偵測的檔案
移到隔離區	移動偵測到的檔案到隔離區。 隔離的檔案無法被執行或開啟，如此可避免被感染的風險。
更改檔名	加入.bd.ren到隱藏的檔案名稱。 如此，您將能夠於您的電腦搜尋並找到(若有)這樣的檔案。 請注意這些隱藏的檔案不是您刻意在系統上隱藏的檔案。這些檔案是被特別的程式或技術所隱藏的。 Rootkit本身並非惡意程式。它們常被用在病毒或間諜程式以避開防毒程式的偵測。

點擊 繼續 以套用指定的動作。

11.1.3. 步驟 3/3 — 檢視結果

當BitDefender 完成修復動作，將會出現一個掃描結果的視窗。



摘要

您可以檢視結果。 若您要了解詳細的掃描資訊，點擊顯示日誌檔案來檢視掃描日誌。



重要

您的系統可能被要求重新啟動以完成您的清理程序。

按下 關閉 關閉視窗。

BitDefender 可能無法解決某些問題

在大部分的情形中，BitDefender 能夠成功地消毒被感染的檔案或是將之隔離。 然而，可能有極少部分的問題無法被解決。

在這種情況下，我們建議您聯絡BitDefender 在網頁www.bitdefender.com的支援團隊。 我們的技術支援代表將會協助您解決您遭遇的問題。

BitDefender 偵測到可疑的檔案

可疑的檔案是被探索式分析歸類被潛在的、沒有正式發布惡意程式碼所感染的檔案。

如果偵測到可疑的檔案，您會被要求將可疑的檔案遞交給BitDefender Lab。 點擊好將這些檔案送交BitDefender Lab做進一步的分析。

11.2. 自訂掃描精靈

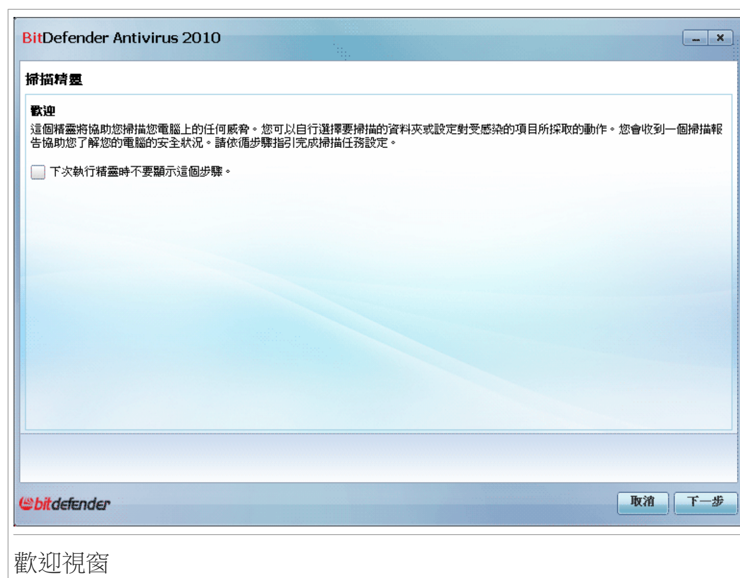
自訂掃描精靈讓您自行建立並執行掃描任務，並可以將它儲存為快速任務。

使用自訂掃描精靈執行自訂掃描任務，依照下列步驟：

1. 在一般模式中，到安全防護標籤。
2. 在快速任務頁面，點擊自定掃描。
3. 依照六步驟指引執行掃描任務。

11.2.1. 步驟 1/6 — 歡迎視窗

這是一個歡迎視窗。



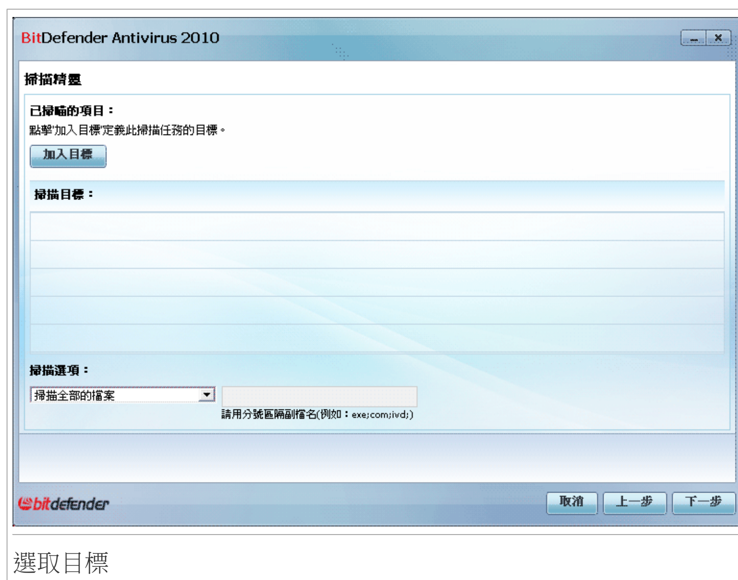
歡迎視窗

如果您想在以後執行精靈時跳過這個畫面・選取下次執行精靈時不要顯示這個步驟核取方塊。

點擊 下一步。

11.2.2. 步驟 2/6 — 選擇目標

您可以在此指定要掃描的檔案及資料夾，以及掃描選項。



選取目標

點擊 加入目標，選取要掃描的檔案或資料夾並點擊 確定。選取的路徑將會出現在掃描目標 欄位。 如果您要變更路徑，只要點擊旁邊的 移除鈕。 點擊移除全部鈕以移除所有加入清單的位置。

當您選取完目標之後，設定掃描選項。 下列可用：

選項	描述
掃描所有檔案	選擇此選項掃描所有在選取的資料夾中的檔案。
只掃描應用程式	只有應用程式檔案將被掃描。代表只有以下副檔名的檔案才會被掃描：.exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml and .nws。
只掃描使用者定義的副檔名	只有被使用者指定的副檔名將會被掃描。這些副檔名必須以"；" 做區隔。

點擊 下一步。

11.2.3. 步驟 3/6 — 選擇動作。

您可以在此指定掃描工具設定和掃描層級。



選擇動作

● 選擇當偵測到受感染或可疑的檔案時執行的動作。 有以下選項可選：

動作	描述
沒有採取動作	在偵測到受感染的檔案時將不會有任何行動。這些檔案將會出現在報告裡。
消毒檔案	從受感染的檔案中移除惡意程式碼。
刪除檔案	立刻刪除受感染的檔案，不經任何警告。
移動檔案到隔離區	移動受感染的檔案到隔離區。 隔離的檔案無法被執行或開啟，如此可避免被感染的風險。

● 選擇當偵測到隱藏的物件(後門程式)執行的動作。 有以下選項可選：

動作	描述
沒有採取動作	在偵測到隱藏檔案時將不會有任何行動。這些檔案將會出現在報告裡。

動作	描述
重新命名	加入.bd.ren到隱藏的檔案名稱。 如此，您將能夠於您的電腦搜尋並找到(若有)這樣的檔案。

● 設置掃描層級。 有三個層級可以選擇。在滑桿上拖曳以選擇適當的防護層級：

掃瞄層級	描述
寬鬆	只有應用程式檔案會被掃描是否有病毒，資源耗用層級為低。
預設	資源耗用層級為中等。所有的檔案都會被掃描是否有病毒或間諜程式。
侵略的	所有檔案(包括檔案封存)，都將會被掃描是否有病毒或間諜程式。隱藏的檔案和程序也包含在掃描中，資源耗用層級較高。

進階的使用者可能會想設置BitDefender 所提供的掃描設定，掃描器可以設置成只掃描特定的惡意程式威脅，這可能大量的減低掃描時間和資源耗用。

拖曳滑桿選擇自訂然後點擊自訂層級鈕。 一個新的視窗將會出現。 指定您要掃描的惡意程式類型，選擇適當的選項：

選項	描述
掃描病毒	掃描已知病毒。 BitDefender也能夠偵測到不完整的病原體，因此能夠移除您系統內的可能威脅。
掃描廣告程式	掃描廣告程式威脅。被偵測到的檔案將被當成受感染的檔案。如果這個選項啟動時，包含廣告元件的軟體將無法運作。
掃描間諜程式	掃描已知的間諜程式。被偵測到的檔案將被當成受感染的檔案。
掃描應用程式	掃描可能會被利用為間諜工具的正當程式。
掃描撥號程式	掃描高收費陷阱的撥號程式。這些被掃描到的檔案將被當成受感染的檔案。如果這個選項啟動時，包含這類型撥號程式的軟體將無法運作。
掃描rootkits	掃描隱藏的物件，一般統稱rootkits。
掃描鍵盤紀錄程式	掃描紀錄鍵盤輸入的惡意程式。

點擊 確定 關閉視窗。

點擊 下一步。

11.2.4. 步驟 4/6 - 額外的設定

在掃描開始之前，可以使用額外的選項：



額外的設定

- 要將您的自訂任務儲存以供未來使用，選取在一般使用者介面顯示這個任務核取方塊並輸入名稱魚編輯欄位。

  任務將會出現在安全防護標籤中的快速任務，也會出現於 進階模式> 病毒防護> 病毒掃描。
- 要在掃描完成後關機，選取掃描完成且沒有找到威脅時關機核取方塊。

點擊開始掃描。

11.2.5. 步驟 5/6 — 進行掃描

BitDefender 將會開始掃描選擇的項目：



掃瞄中



註

掃描程序將依它的複雜程度而需花費一些時間。 您可以在系統工具列看見 掃描程序圖示。

11.2.6. 步驟 6/6 - 檢視結果

當BitDefender 完成修復動作，將會出現一個掃描結果的視窗：



摘要

若您要了解詳細的掃描資訊，點擊顯示日誌檔案來檢視掃描日誌。



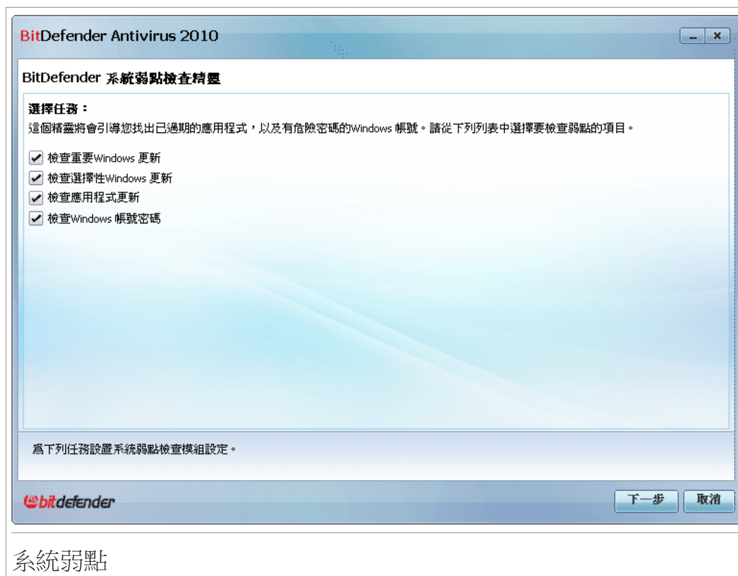
重要
您的系統可能被要求重新啟動以完成您的清理程序。

按下 關閉 關閉視窗。

11.3. 系統弱點檢查精靈

這個精靈檢查系統弱點並協助您修復它們。

11.3.1. 步驟 1/6 - 選擇要檢查的系統弱點



系統弱點

點擊下一步以檢查系統已選的弱點。

11.3.2. 步驟 2/6 – 系統弱點檢查



系統弱點檢查

等待BitDefender 完成系統弱點檢查。

11.3.3. 步驟 3/6 - 更新Windows



Windows 更新

您可以查看您尚未安裝的Windows更新清單。 點擊安裝所有系統更新以安裝所有可用的更新。

點擊 下一步。

11.3.4. 步驟 4/6 – 更新應用程式



應用程式

您可以查看BitDefender檢查的的應用程式清單及他們的更新狀態。 若應用程式未更新，請點擊連結以更新到最新版本。

點擊 下一步。

11.3.5. 步驟 5/6 – 更改危險的密碼



使用者密碼

您可以檢視您電腦中的Windows使用者帳戶清單，以及他們的密碼防護層級。 密碼可能為安全 (難以猜測) 或 危險 (容易被猜出)。

點擊修復以更改不安全的密碼。 將會開啟一個新的視窗。



變更密碼

選擇修復此事件的方法：

- 強制使用者在下一次登入時變更密碼. BitDefender將提示使用者在下次登入Windows時更改密碼。
- 變更使用者密碼. 您必須在文字框輸入新的密碼。 確認通知用戶密碼已變更。



註

使用大小寫混用、數字或特殊符號（例如#、$或@），以加強密碼。 您可以搜尋網路以了解更多關於安全密碼的資訊。

點擊確定以變更密碼。

點擊 下一步。

11.3.6. 步驟 6/6 - 檢視結果



結果

點擊關閉。

一般檢視模式

12. 狀態顯示表

狀態顯示表標籤提供關於安全防護的相關資訊，並允許您修復擱置的事件。



狀態顯示表

狀態顯示表包含包含了幾個頁面：

● 整體狀態 — 提示可能影響電腦安全的事件並協助您修復他們。 有驚嘆號的紅色圓圈與修復所有事件按鈕。點擊按鈕開始修復所有事件精靈。

● 詳細狀態 - 以簡單的句子讓您了解主要模組的狀態，並配合下列圖示：

打勾的綠色圈圈： 沒有事件影響安全狀態。 您的電腦已受到防護。

有驚嘆號的灰色圈圈： 這個模組的元件沒有被監控。所以沒有它們的安全狀態相關訊息。 可能有些特殊的事件與這個模組相關。

有驚嘆號的紅色圈圈： 有影響您系統安全的事件。 重大的事件需要立即的關注，非重大的事件也需要盡快被解決。

點擊模組名稱以檢視更多有關狀態的訊息，以及設置元件的狀態追蹤。

● 使用設定檔 - 表示目前所選用來作為提供相關功能連結的設定檔。

□當 典型設定檔被選取，立刻掃描鈕將可以用來執行系統掃描並開啟病毒防護掃描精靈。 整個系統都將會被掃描，除了檔案封存。在預設設置中，除了後門程式之外的惡意程式都將會被掃描。

- 當選擇遊戲玩家設定檔，開啟/關閉遊戲模式讓您可以啟動/停用 遊戲模式。 遊戲模式能夠暫時地變更防護設定，將系統運行的影響減至最低。
- 當自訂設定檔被選取，立即更新鈕將會開始立即更新。 您可以在新開啟的視窗檢視更新狀況。

如果您想切換或變更使用設定檔，點及設定檔並依照設置精靈操作。

13. 病毒防護

BitDefender的安全防護模組能夠協助您的電腦免受病毒威脅並且能夠隨時自動更新。請點擊病毒防護標籤，進入病毒防護模組。



病毒防護

病毒防護模組包含兩個部分：

- 狀態區域 - 顯示所有受監控項目的狀態並可以選擇要監控的項目。
- 快速任務 - 在這裡您可以找到重要的安全任務連結：立即更新、掃描我的文件、系統掃描、深度掃描和自訂掃描。

13.1. 狀態區

您可以在狀態區檢視完正的安全模組元件清單和它們的狀態。透過監控安全防護模組，BitDefender 會讓您知道不是只有設置設定會影響您的電腦安全，忘了執行重要的任務也有負面影響。

元件目前的狀態以簡單的句子和以下的圖示表示：

- 打勾的綠色圈圈： 沒有事件影響這個元件。
- 有驚嘆號的紅色圈圈： 有事件影響這個元件。

描述事件的句子顯示為紅色。 點擊修復鈕以修復對應的事件。 如果有一個問題不能被修復，請跟隨精靈的指示來修復。

13.1.1. 設置狀態追蹤

若要BitDefender監控檔案加密模組，點擊設置狀態追蹤並點選啟動警示通知方塊。



重要
要確保您的電腦完整的受到防護，請啟動追蹤所有元件並修復所有事件。

下列是BitDefender可追蹤的安全元件狀態：

- 病毒防護 - BitDefender監控病毒防護的兩個元件：即時防護及手動掃描。 這個元件最常見的事件已列在下方表格。

事件	描述
即時防護已停用	存取的檔案、或者應用程式執行的程式沒有被掃描。
這台電腦從未掃描病毒	從未執行過手動掃描以檢查電腦中是否有惡意程式。
上一次系統掃描在完成前就被終止	全系統掃描開始但並未完成。
病毒防護在危險狀態	即時防護已停用且系統掃描逾期。

- 更新 - BitDefender監控惡意呈是特徵碼是否在最新狀態。 這個元件最常見的事件已列在下方表格。

事件	描述
自動更新已停用	您的惡意程式特徵碼並沒有自動的定期更新。
更新已有x天未被執行	您的惡意程式特徵碼已過期。

13.2. 快速任務

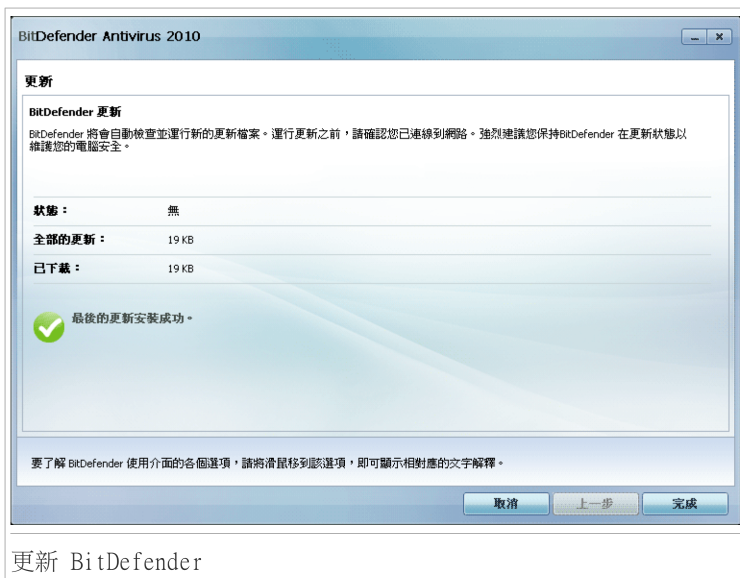
這裡您可以找到最重要的安全任務連結。

- 立即更新 - 立刻執行更新。
- 系統掃描 - 開啟一個電腦的完整掃描。要設置額外的手動掃描選項，點擊並選取一個不同的掃描任務：掃描我的文件或深度系統掃描。
- 自訂掃描 - 開啟一個讓您能夠自行建立並執行掃描的精靈。

13.2.1. 更新 BitDefender

每一天都有新的惡意程式被發現及識別。這就是為什麼 BitDefender 需要保持最新的病毒特徵碼是非常重要的。預設上，BitDefender 是每個小時自動檢查更新。

當您啟動您的電腦系統時，BitDefender已預設檢查是否有更新，之後每小時都會持續的檢查更新。 然而，如果您要執行更新，點擊立即更新鈕。 更新程序會立即啟動並且出現下列視窗：



更新 BitDefender

您可以在此視窗檢視更新狀態。

更新程序表示檔案會漸進地更新替換。如此更新程序不會影響產品性能，同時所有的弱點將被排除。

如果您想要關閉此視窗，請點擊取消。 然而，這並不會終止更新程序。



註
如果您是利用撥接方式連線到網際網路，建議您定期地更新 BitDefender 以獲得最好的防護效果。

如果需要，請重新啟動電腦。. 若有重大的更新，您將會被要求重新啟動您的電腦。點擊重新啟動以重新啟動您的電腦。

假如您想要稍後再重新啟動您的系統，請點擊好。 建議您盡快重新啟動您的系統。

13.2.2. 使用BitDefender掃瞄

要掃描您電腦中的惡意程式，請點擊對應按鈕執行特定的掃描任務。 您可以在下表檢視可用的掃描任務以及簡述：

任務	描述
系統掃描	掃描整個系統，資料封存除外。 在預設的設定中，它將掃描除了後門程式之外的所有惡意程式類型。
我的文件掃描	利用這個任務掃描重要的使用者資料夾：我的文件，桌面和開始功能表。 這麼做可以保障您的檔案安全並且提供安全的環境運作應用程式。
深度系統掃描	掃描整個系統。 在預設的設置中，它能夠掃描您電腦中所有種類的惡意威脅。
自訂掃瞄	使用這個任務以選擇掃描特定的檔案或資料夾。



註

深度系統掃瞄 與 全系統掃瞄 是針對系統整體的分析任務，所以會需要較長的時間，我們建議您可以以低優先率執行此任務，甚至在您的系統閒置時更好。

當您執行系統掃描、深度系統掃描或我的文件掃描，將會出現病毒防護掃描精靈。 依照三步驟指引執行掃描任務。 要了解更多資訊，請參考 “病毒掃描精靈” (p. 46)。

當您執行自訂掃描，自訂掃描精靈京會引導您完成掃描程序。 依照六步驟的引導以掃描特定的資料夾或檔案。 要了解更多資訊，請參考 “自訂掃描精靈” (p. 49)。

14. 反網路釣魚

BitDefender的反網路釣魚確保您透過Internet Explorer或Firefox的所有網頁存取都是安全的。 要進入反網路釣魚模組，請點擊反網路釣魚標籤。



反網路釣魚

反網路釣魚模組包含兩個部分：

- 狀態區 - 顯示反網路釣魚模組目前的狀態，以及讓您能夠啟動/停用模組活動追蹤。
- 快速任務 - 在這裡您可以找到重要的安全任務連結：立即更新、掃描我的文件、系統掃描和深度系統掃描。

14.1. 狀態區

元件目前的狀態以簡單的句子和以下的圖示表示：

- 打勾的綠色圈圈： 沒有事件影響這個元件。
- 有驚嘆號的紅色圈圈： 有事件影響這個元件。

描述事件的句子顯示為紅色。 點擊修復鈕以修復對應的事件。

這個模組常會見到的事件是反網路釣魚已停用。 這代表反網路釣魚沒有在下列支援的任何一個應用程式啟動：Internet Explorer、 Mozilla Firefox、 Yahoo! 即時通或Windows Live Messenger。

14.2. 快速任務

這裡您可以找到最重要的安全任務連結。

- 立即更新 - 立刻執行更新。
- 系統掃描 — 執行一個完整的系統掃描(除了資料封存)。
- 深度系統掃瞄 — 執行一個針對您的電腦系統的完整掃瞄(包含資料封存)。

14.2.1. 更新 BitDefender

每一天都有新的惡意程式被發現及識別。這就是為什麼 BitDefender 需要保持最新的病毒特徵碼是非常重要的。預設上，BitDefender 是每個小時自動檢查更新。

當您啟動您的電腦系統時，BitDefender已預設檢查是否有更新，之後每小時都會持續的檢查更新。 然而，如果您要執行更新，點擊立即更新鈕。 更新程序會立即啟動並且出現下列視窗：



更新 BitDefender

您可以在此視窗檢視更新狀態。

更新程序表示檔案會漸進地更新替換。如此更新程序不會影響產品性能，同時所有的弱點將被排除。

如果您想要關閉此視窗，請點擊取消。 然而，這並不會終止更新程序。



註
如果您是利用撥接方式連線到網際網路，建議您定期地更新 BitDefender 以獲得最好的防護效果。

如果需要，請重新啟動電腦。. 若有重大的更新，您將會被要求重新啟動您的電腦。點擊重新啟動以重新啟動您的電腦。

假如您想要稍後再重新啟動您的系統，請點擊好。 建議您盡快重新啟動您的系統。

14.2.2. 使用BitDefender掃瞄

要掃描您電腦中的惡意程式，請點擊對應按鈕執行特定的掃描任務。 您可以在下表檢視可用的掃描任務以及簡述：

任務	描述
系統掃描	掃描整個系統，資料封存除外。 在預設的設定中，它將掃描除了後門程式之外的所有惡意程式類型。
深度系統掃描	掃描整個系統。 在預設的設置中，它能夠掃描您電腦中所有種類的惡意威脅。



註
深度系統掃瞄 與 全系統掃瞄 是針對系統整體的分析任務，所以會需要較長的時間，我們建議您可以以低優先率執行此任務，甚至在您的系統閒置時更好。

當您執行系統掃描或深度系統掃描，將會出現病毒防護掃描精靈。 依照三步驟指引執行掃描任務。 要了解更多資訊，請參考 “病毒掃描精靈” (p. 46)。

15. 系統弱點

BitDefender的弱點檢查模組能夠幫助您更新電腦中的重要軟體。 請點擊系統弱點標籤，監控並修復您的系統弱點。



系統弱點

弱點檢查模組包含兩個部分：

- 狀態區 - 顯示系統弱點檢查模組目前的狀態，以及讓您能夠啟動/停用模組活動追蹤。
- 快速任務 - 您可以在此找到系統弱點檢查精靈的連結。

15.1. 狀態區

元件目前的狀態以簡單的句子和以下的圖示表示：

- 打勾的綠色圈圈： 沒有事件影響這個元件。
- 有驚嘆號的紅色圈圈： 有事件影響這個元件。

描述事件的句子顯示為紅色。 只要在對應的事件點擊修復或安裝即可修復事件。

這個元件最常見的事件已列在下方表格。

任務狀態	描述
系統弱點檢查已停用	BitDefender 沒有檢查潛在的系統弱點，例如缺少的Windows更新、應用程式更新或危險的密碼。
偵測到多個系統弱點	BitDefender 找到缺少的Windows/應用程式更新或危險的密碼。
重要的Microsoft更新	重大的Microsoft 更新可用但沒有安裝。
其他Microsoft更新	非重大的Microsoft 更新可用但沒有安裝。
Windows自動更新已停用	Windows 安全性更新並不會在可用時便自動安裝。
應用程式 (過期)	更新版本的應用程式 可用但尚未安裝。
使用者 (危險的密碼)	一個使用者的密碼很容易被惡意的駭客或軟體入侵。

15.2. 快速任務

有一個可用的任務：

- 系統弱點掃描 – 啟動一個可以檢查系統弱點並加以修復的精靈。

系統弱點檢查會監控所有Microsoft Windows產品的更新以及Windows的帳戶密碼，保持您的作業系統在最新的狀態。

要檢查電腦中的系統弱點，點擊系統弱點掃描並依循“系統弱點檢查精靈” (p. 56)。

16. 網路

網路模組提供您管理每一台家庭電腦中安裝的BitDefender。 進入網路模組，請點擊網路標籤。



網路

要管理您家庭電腦安裝的BitDefender，請您依照下列步驟：

1. 在您的電腦加入BitDefender家庭網路。 加入網路，為家庭網路管理設置一個管理者密碼。
2. 使用您想管理與加入網路的電腦，並設定密碼。
3. 回到您的電腦，並新增這些您想管理的電腦。

16.1. 快速任務

一開始只有一個按鈕可使用。

- 啟動網路 - 提供您設定網路密碼以建立並進入網路。

加入網路之後，將出現其他的按鈕。

- 停用網路 - 提供您離開網路。
- 加入電腦 - 您可新增電腦至您的網路。
- 掃描全部 - 提供您同時掃描所有管理中的電腦。
- 全部更新 - 提供您同時更新所有管理中的電腦。

- 全部註冊 - 提供您同時註冊所有管理中的電腦。

16.1.1. 加入BitDefender 網路

要加入BitDefender 家庭網路，請依照下列步驟：

1. 點擊啟動網路。 將提示您設置家庭管理密碼。

BitDefender
輸入家庭網路的密碼
加入或建立網路需要輸入密碼，可以保護您的電腦不被任意變更。
密碼：
請再次輸入密碼：
確定 取消

設置密碼

2. 在兩個文字框中輸入相同密碼。
3. 按下確定。

您可以在網路地圖上看到電腦名稱。

16.1.2. 加入電腦至BitDefender 網路

加入電腦至BitDefender 網路前，您必須先在每一台電腦設置BitDefender家庭管理密碼。

要加入電腦至BitDefender 網路，請依照下列步驟：

1. 點擊加入電腦。 將提示您輸入本地家庭管理密碼。

BitDefender
請輸入您設定給家庭管理的密碼。
密碼
不要再顯示此訊息。
確定 取消

輸入密碼

2. 輸入家庭管理密碼，並點擊確定。 將會開啟一個新的視窗。



加入電腦

您可以檢視網路中的電腦清單。 小圖示的意義如下：

顯示一台線上電腦，但未安裝BitDefender。

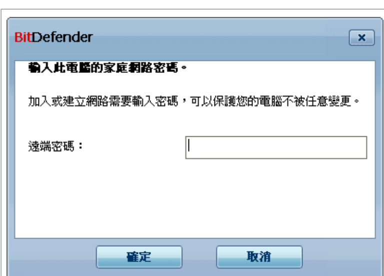
顯示一台線上電腦，已安裝BitDefender。

顯示一台離線電腦，已安裝BitDefender。

3. 您可以選擇以下動作：

- 從清單中選擇要加入的電腦名稱。
- 在對應欄位輸入要加入的電腦IP位置或電腦名稱。

4. 點擊加入。 將提示您輸入電腦的家庭管理密碼。



密碼確認

5. 輸入該電腦的家庭管理密碼。

6. 按下確定。 若密碼輸入正確，該電腦將出現在網路地圖上。



註
您最多可以加入五台電腦至網路地圖。

16.1.3. 管理BitDefender網路

只要您成功建立一個BitDefender家庭網路，您就可以管理所有電腦中的BitDefender。



網路區域

移動游標至網路地圖上的電腦，您可以查看該電腦的資訊概要(名稱、IP位置、系統安全事件數量、BitDefender註冊狀態)。

在網路地圖上的電腦名稱點擊右鍵，您可以查看所有能在遠端電腦上執行的管理任務。

- 從家庭網路移除電腦

  讓您能夠從網路中移除電腦。

- 在這台電腦註冊BitDefender

  讓您能夠以授權序號註冊BitDefender。

- 設置設定密碼於遠端電腦

  讓您能夠建立密碼以限制變更BitDefender的設定。

- 執行手動掃描任務

  讓您能夠在遠端電腦上執行手動掃描，您可以執行下列任務：我的文件掃描、系統掃描或深度系統掃描。

- 在這台電腦上修復所有事件

  讓您透過修復所有事件 精靈以修復可能影響您電腦安全的事件。

- 檢視歷史/事件

  讓您使用歷史&事件 模組。

- 立即更新

  開始更新安裝在此電腦上的BitDefender 產品。

- 設定此電腦為此網路的更新伺服器

  讓您能夠設置這台電腦為整個網路中的BitDefender更新伺服器。 使用這個選項將會減少網路傳輸，因為只有一台電腦會連上網路下載更新。

在執行特定電腦的任務以前，將提示您輸入本地家庭管理密碼。



輸入密碼

輸入家庭管理密碼，並點擊確定。



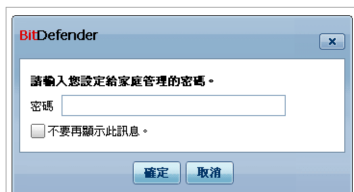
註

若您要執行多個任務，您可以選擇這段期間不要再顯示這個訊息。 這樣，這段期間將不會再提示您輸入密碼。

16.1.4. 掃描所有電腦

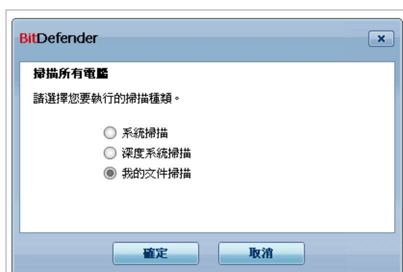
要掃描所有管理中的電腦，請依照下列步驟：

1. 點擊掃描全部。 將提示您輸入本地家庭管理密碼。



輸入密碼

2. 選擇一個掃描類型。
- 系統掃描 — 執行一個完整的系統掃描(除了資料封存)。
- 深度系統掃瞄 — 執行一個針對您的電腦系統的完整掃瞄(包含已資料封存)。
- 掃描我的文件 — 執行一個針對我的檔案資料夾的快速掃描。



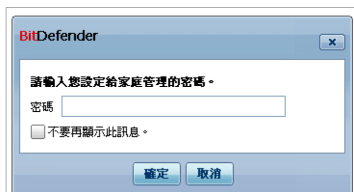
選擇掃描類型

3. 按下確定。

16.1.5. 更新所有電腦

要更新所有管理中的電腦，請依照以下步驟：

1. 點擊全部更新。 將提示您輸入本地家庭管理密碼。



輸入密碼

2. 按下確定。

16.1.6. 註冊所有電腦

要註冊所有管理中的電腦，請依照以下步驟：

1. 點擊註冊全部。 將提示您輸入本地家庭管理密碼。

輸入密碼

2. 輸入您想註冊的序號。

全部註冊

3. 按下確定。

進階檢視模式

17. 一般

一般模組提供有關BitDefender 的動作以及系統的相關資訊。 您也可以在此變更BitDefender 的整體行動。

17.1. 狀態顯示表

要檢視是否有事件影響您的電腦，以及產品活動統計及註冊狀態，到進階模式中的一般>狀態顯示表。

狀態顯示表

狀態顯示表包含包含了幾個頁面。

- 整體狀態 提示可能影響電腦安全的事件。
- 統計數據－顯示重要的BitDefender動作相關數據。
- 總覽 — 檢視更新狀態、您的帳號狀態以及註冊相關資訊。
- 檔案區－表示BitDefender所掃描到的惡意程式數量變化，長度代表時間區段內發現的密度。

17.1.1. 整體狀態

您可以在此看到影響您電腦安全的事件數量。 要移除所有威脅，點擊修復所有事件。 這將會開始修復所有事件精靈。

要設置被BitDefender 病毒防護2010堆中的模組，點擊設置狀態追蹤。 一個新的視窗將會出現：



設置狀態警示

如果您想要BitDefender監控元件，勾選元件的啟動警示核取方塊。 下列是BitDefender可追蹤的安全元件狀態：

- 病毒防護 - BitDefender監控病毒防護的兩個元件：即時防護及手動掃描。 這個元件最常見的事件已列在下方表格。

事件	描述
即時防護已停用	存取的檔案、或者應用程式執行的程式沒有被掃描。
您從未掃瞄您電腦中的惡意程式	從未執行過手動掃描以檢查電腦中是否有惡意程式。
上一次系統掃描在完成前就被終止	全系統掃描開始但並未完成。
病毒防護在危險狀態	即時防護已停用且系統掃描逾期。

- 更新 - BitDefender監控惡意呈是特徵碼是否在最新狀態。 這個元件最常見的事件已列在下方表格。

事件	描述
自動更新已停用	您的惡意程式特徵碼並沒有自動的定期更新。
更新已有x天未被執行	您的惡意程式特徵碼已過期。

- 反網路釣魚 - BitDefender監控反網路釣魚狀態。 如果沒有在所有支援的應用程式上啟動，將會報告反網路釣魚已停用。
- 系統弱點檢查 - BitDefender追蹤系統弱點檢查功能。系統弱點檢查讓您了解是否有未安裝的Windows更新、應用程式更新、以及您的密碼安全度。

  這個元件最常見的事件已列在下方表格。

任務狀態	描述
系統弱點檢查已停用	BitDefender 沒有檢查潛在的系統弱點，例如缺少的Windows更新、應用程式更新或危險的密碼。
偵測到多個系統弱點	BitDefender 找到缺少的Windows/應用程式更新或危險的密碼。
重要的Microsoft更新	重大的Microsoft 更新可用但沒有安裝。
其他Microsoft更新	非重大的Microsoft 更新可用但沒有安裝。
Windows自動更新已停用	Windows 安全性更新並不會在可用時便自動安裝。
應用程式 (過期)	更新版本的應用程式 可用但尚未安裝。
使用者 (危險的密碼)	一個使用者的密碼很容易被惡意的駭客或軟體入侵。



重要

要確保您的電腦完整的受到防護，請啟動追蹤所有元件並修復所有事件。

17.1.2. 統計數據

如果您想持續追蹤BitDefender的動作，統計數據頁面會是個好開始。 您可以檢視下列項目：

項目	描述
已掃瞄的檔案	表示上一次掃描所檢查的檔案數量。
已消毒的檔案	表示上一次掃描成功消毒的檔案數量。

項目	描述
已偵測到被感染的檔案	表示在上一次掃描時在您的系統所發現的受感染檔案數量。
上一次系統掃瞄	表示您上一次何時更新。 若上一次掃描為一週以前，請盡快掃描您的電腦。 要掃描整台電腦，到病毒防護，病毒掃描標籤頁，並執行系統掃描程序。
下一次掃描	表示下次您的電腦要被掃描的時間。

17.1.3. 總覽

您可在此檢視更新狀態、帳號狀態、註冊與授權資訊。

項目	描述
上次更新	表示您的帳號最後何時更新。 請執行更新以擁有最完善的防護。
BitDefender 帳號	顯示用來存取線上帳戶的電子郵件位址，您可以使用它存取您的線上帳戶以重新取得您遺失的BitDefender授權序號、得到BitDefender支援及其他服務。 您必須建立一個BitDefender帳號以啟動產品。 要了解更多資訊，請參閱"註冊與我的帳號" (p. 41)。
註冊。	顯示您的授權序號及狀態。若您的序號已過期，請續購或升級產品以保護您的系統安全。
到期	顯示授權序號到期的天數。 若您的序號已快要到期，請註冊新的授權序號。 要購買新序號或是續購，點擊畫面下方的購買連結。

17.2. 設定

要設置並管理一般設定，請在進階模式選擇一般>設定。



一般設定

在這裡可以設定所有 BitDefender 喜好。預設上，BitDefender 會在視窗啟動時被載入，並執行最小化在系統工具列上。

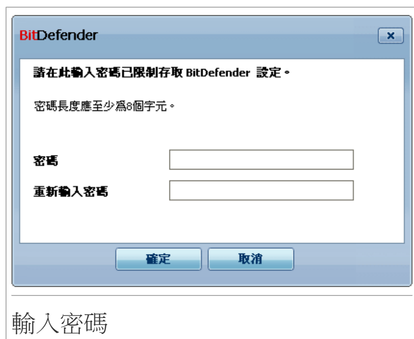
17.2.1. 一般設定

- 啟動密碼保護 — 此選項為了保護 BitDefender 管理主控台的設定。



註
如果您不是此電腦唯一擁有管理權限的人，建議您設定密碼保護您的 BitDefender 設定。

如果您選擇了此選項，將會出現下一個視窗：



輸入密碼

在密碼欄位上，輸入密碼，在重新輸入密碼欄位上，重新輸入密碼，並點擊確定。

一旦您設了密碼，每次您要變更BitDefender設定時，您都會被要求輸入密碼。 其他的系統管理者(如果有)若要變更設定也是需要此密碼。



重要

如果忘記密碼，您必須修復此軟體才可進行 BitDefender 的設定。

- 顯示BitDefender消息 (安全通知) - 由 BitDefender 伺服器寄送關於病毒疫情擴散的即時安全通知。
- 顯示彈出式視窗 (螢幕上的提示) - 在彈出式視窗顯示產品狀態。 您可以設置 BitDefender 只顯示彈出式視窗於新手/一般模式或進階模式。
- 啟動掃描活動列 (螢幕上顯示掃描活動的狀態 — 啟動/關閉掃描活動列。 您可以取消這個核取方塊如果您不想看見掃描活動列。



掃瞄活動列



註

此選項只能被目前的Windows使用者這戶調整。 掃描活動列只會在切換到進階模式時才會出現。

17.2.2. 病毒報告設定

- 寄送病毒報告 — 當您的電腦發現病毒時，寄發病毒報告到 BitDefender 實驗室。 它將協助我們保持病毒疫情擴散的追蹤。

  這份報告不會包含機密資料，如：您的姓名、IP 位址或其他，也不會被使用在商業目的上。這個資訊只包含病毒名稱，並且僅僅用來建立統計報告。

- 啟動 BitDefender 疫情擴散偵測 - 將潛在病毒疫情擴散報告寄送到 BitDefender 實驗室。

  這份報告將不包含機密資料，如：您的姓名、IP 位址或其他，而且此份資料不會被使用在商業目的上。這個資訊只包含潛在病毒並且僅僅用來偵測新的病毒。

17.3. 系統資訊

BitDefender 使您從單一個地方便能夠檢視開機時所有的系統設定以及登錄執行的應用程式。如此，您可以監控所有系統的活動並能夠辨識感染的發生。

要獲得系統資訊，請在進階模式選擇一般>系統資訊。



系統資訊

這個清單包含所有被載入的項目，當系統啟動時，這些項目會被不同應用程式所載入。

可用三個按鈕：

- 還原－變更目前的檔案關聯至預設值。 只在檔案關聯設定可用。
- 到 — 開啟您所選擇項目的視窗（如：登錄）



註
隨著所選的項目不同， 到按鈕不一定會出現。

- 重新整理 — 重新整理 系統資訊 頁面。

18. 病毒防護

BitDefender保護您的電腦對抗所有惡意程式的威脅 (病毒、間諜程式、木馬程式及其他)。 BitDefender 的安全防護可分為二類：

- 即時防護－保護您的系統不受新進入的惡意程式威脅。 舉例來說，當您打開它的時候， BitDefender 將會掃描您正在開啟的 Word 檔案，以及您接收中的電子郵件。



註
即時防護同時也包括了存取掃描－當檔案被使用者存取時，就會受到掃描。

- 手動掃描－允許掃描並移除已在您的系統的惡意程式。 這是由使用者啟動的典型掃描－您手動選擇要掃描的磁碟、資料夾或檔案，而BitDefender 進行掃描。 您可以建立個人化的例行掃描時程。

18.1. 即時防護

BitDefender提供持續性的即時防護，透過掃描存取的檔案、電子郵件訊息和即時通訊應用程式(ICQ, NetMeeting, Yahoo即時通, MSN Messenger)，以對抗多種類的惡意程式威脅。 BitDefender 反網路釣魚能夠在您瀏覽可能帶有竊取個人訊息的網頁時，警告您潛在的網路釣魚網站。

要設置即時防護及BitDefender反網路釣魚，請在進階模式選擇病毒防護>防禦。



即時防護

您可以檢視即時防護是已啟動或停用。 如果您想變更即時防護狀態，選取或清除對應的核取方塊。



重要

為了防止病毒感染您的系統，請保持即時防護 啟動。

要開始系統掃瞄，點擊立即掃瞄。

18.1.1. 設置防護層級

您可以選擇最適合您安全需求的防護層級。拖曳滑桿設定合適的防護層級。

有三種防護層級：

防護層級	描述
寬鬆	涵蓋基本的安全需求。資源耗用層級非常低。

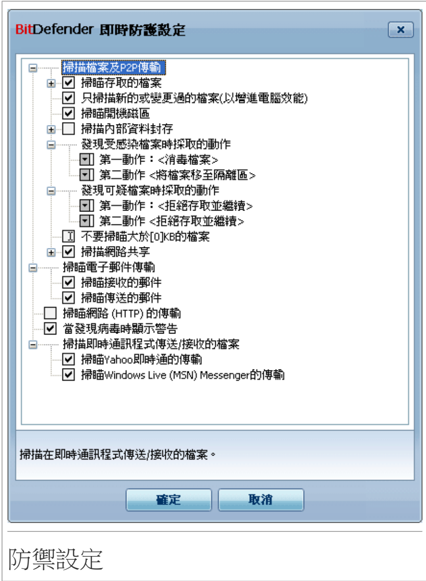
防護層級	描述
	只有應用程式和接收的電子郵件會被掃描。除了傳統的特徵掃描外，也使用啟發式的分析。受感染的檔案將採取以下的動作：消毒檔案/搬移檔案到隔離區。
預設	提供標準的安全防護。資源耗用層級較低。 所有檔案、接收及傳送的電子郵件都會被掃描是否有病毒或間諜程式。除了傳統的特徵掃描外，也使用啟發式的分析。受感染的檔案將採取以下的動作：消毒檔案/搬移檔案到隔離區。
侵略的	提供較高的安全防護。耗用資源層級中等。 所有檔案、接收&傳送的電子郵件及網站的傳輸都會被掃描是否有病毒或間諜程式。除了傳統的特徵掃描外，也使用啟發式的分析。受感染的檔案將採取以下的動作：消毒檔案/移動檔案至隔離區。

如果您想要回復到預設層級，點擊 預設層級。

18.1.2. 自訂防護層級

進階的使用者可以使用 BitDefender 所提供的掃描設定。掃描器中可以設定指定特定的副檔名、目錄或您所知道無害的檔案。這將會減少掃描時間並加快您系統掃描的反應時間。

您可以自訂 即時防護，點擊 自訂層級。將會出現下一個視窗：



防禦設定

掃描的選項以可擴展的選單方式呈現，非常相似於 Windows 檔案總管。 點擊 "+" 的小方框以展開選項或點擊 "-" 的小方框關閉選項。



註

您會注意到雖然一些掃描選項前面出現 "+"，但卻無法被展開。這是因為這些選項尚未被選取。您會注意到，如果您選擇了這些選項，則其細項即可被展開。

- 掃描存取的檔案及點對點的傳輸選項 — 掃描被存取的檔案及透過即時傳訊軟體溝通的應用程式 (ICQ、NetMeeting、Yahoo 即時通、MSN Messenger)。選擇您所要掃描的檔案型態。

選項		描述
掃描存取的檔案	掃描所有檔案	所有存取的檔案都將被掃描，不管其型態為何。
	只掃描應用程式	只有應用程式檔案將被掃描。代表只有以下副檔名的檔案才會被掃描：.exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml;

選項		描述
		.xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml and .nws。
	掃描使用者定義的副檔名	只有被使用者指定的副檔名將會被掃描。這些副檔名必須以"；" 做區隔。
	掃描危險軟體	掃描危險軟體。 被偵測掃描的危險軟體將被當成受感染的檔案。如果這個選項啟動時，包含廣告元件的軟體將無法運作。 選取掃描跳過撥號程式及應用程式 或 掃描跳過鍵盤紀錄程式 以排除這些檔案類型。
只掃描新的與變更過的檔案		只掃描沒有被掃瞄過的或是被更動過的檔案。藉由選擇此選項，您可以增進產品的系統效能，但會降低安全層次。
掃描開機磁區		掃描系統開機磁區。
掃描內部資料封存		被存取的資料封存將被掃描。當這個選項啟動時，電腦將會變慢。 您可以設定檔案封存的掃描大小上限(以KB計，輸入0代表您要掃描所有的檔案封存)，以及檔案封存的掃描深度上限。
第一動作		從下拉式選單選擇當遇到受感染及可疑檔案時，第一動作所要採取的行動。
	拒絕存取並繼續	當偵測到受感染的檔案，對它的存取動作也將被禁止。
	消毒檔案	從受感染的檔案中移除惡意程式碼。
	刪除檔案	立刻刪除受感染的檔案，不經任何警告。
	移動檔案到隔離區	移動受感染的檔案到隔離區。 隔離的檔案無法被執行或開啟，如此可避免被感染的風險。
第二動作		從下拉式選單選擇當遇到受感染的檔案時，所要採取的第二動作。(當第一動作失敗時)
	拒絕存取並繼續	當偵測到受感染的檔案，對它的存取動作也將被禁止。
	刪除檔案	立刻刪除受感染的檔案，不經任何警告。
	移動檔案到隔離區	移動受感染的檔案到隔離區。 隔離的檔案無法被執行或開啟，如此可避免被感染的風險。

選項		描述
不要掃描大於 [x] Kb 檔案		輸入要被掃描的最大檔案大小。如果大小為 0Kb， 代表所有檔案將被掃描，而不管這些檔案的大小。
掃描網路共用檔案	掃描所有檔案	所有從網路存取的檔案都將被掃描，不管其型態為何。
	只掃描應用程式	只有應用程式檔案將被掃描。代表只有以下副檔名的檔案才會被掃描：.exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml and .nws。
	掃描使用者定義的副檔名	只有被使用者指定的副檔名將會被掃描。這些副檔名必須以"；" 做區隔。

- 掃描電子郵件傳輸 — 掃描電子郵件的傳輸。

  有以下選項可選：

選項	描述
掃描接收的電子郵件	掃描所有接收的電子郵件訊息。
掃描傳送的電子郵件	掃描所有傳送的電子郵件訊息。

- 掃描 Http 傳輸 — 掃描 Http 傳輸。
- 當發現病毒時提出警告 — 在檔案或電子郵件中發現病毒時，開啟一個警示視窗。

  一個受感染的警告視窗將包含病毒名稱、發現的路徑、BitDefender 所採取的行動及一個連結到 BitDefender 的網站，在那裡您可以得到更多關於此病毒的資訊。在一個受感染的電子郵件警示視窗裡也包含了寄件者及收件者的資訊。

  當偵測到一個可疑的檔案時，您可以從警告視窗裡開啟一個精靈，它將協助您寄送檔案到 BitDefender 實驗室進行分析。您可以輸入您的電子郵件位址以得到這個報告的相關資訊。

- 掃描經由即時通訊接收或傳送的檔案. 要掃描經由Yahoo 即時通或Windows Live Messenger接收或傳送的檔案，請選取對應的核取方塊。

按 確定 儲存這個設定並關閉視窗。

18.1.3. 設置主動病毒管控設定

BitDefender主動病毒管控(AVC)提供您針對擁有未發佈的特徵的惡意程式的防護。 它將持續監控並分析在您電腦上運行的應用程式行為，當應用程式出現可疑行為時提出警告。

AVC可以設置以警示並提醒您有應用程式正在嘗試執行類似惡意的行為。



BitDefender 主動病毒管控警示

如果您知道並信任被偵測到的應用程式，點擊允許。

如果您想要立刻關閉這個應用程式，點擊確定。

點選記住此應用程式的動作方塊，BitDefender會在日後記住此動作。 規則被建立後將會列在例外的表格。

要設置主動病毒管控，點擊 BD AVC 設定。



BitDefender AVC 設定

點選對應的方塊以啟動AVC管控。



重要
保持可疑AVC啟動以防護未知的病毒。

若您要AVC在任何應用程式有惡意行為時提醒您，詢問我再採取動作的方塊。

設置防護層級

AVC防護層級會自動隨著即時防護層級變更。 如果不滿意預設的設定，您可以手動設置防護層級。



註
請注意如果您變更了即時防護層級，AVC掃描防護層級會自動隨著變更。 若您將即時防護設為寬鬆，則AVC是停用的。

拖曳滑桿以設定您認為適當的防護層級。

防護層級	描述
重要	嚴格管控所有可能的惡意行為。
預設	偵測率高且可能會有誤判。

防護層級	描述
中	中度監控應用程式，仍可能會有誤判發生。
寬鬆	偵測率較低但是不會有誤判。

管理信任/不信任的應用程式清單。

您可以將應用程式加入到清單，清單中的程式會自動被允許存取。 同樣地，您可以將應用程式加到不信的清單，BitDefender AVC將會自動阻擋它們。

建歷過規則的應用程式將會列在例外的表格。 每一個規則將會顯示應用程式的路徑與設定的動作。

要管理清單，使用位在上方的按鈕：

- Add - 加入新項目到清單。
- 移除 - 從清單移除項目。
- 編輯 - 編輯應用程式的規則。

18.1.4. 停用即時防護

如果您想要停用即時防護，將會出現一個警告視窗。 您可以從視窗選擇您要停用即時防護的時間長度。您可以選擇：5分鐘、15分鐘、30分鐘、一個小時、永久停用、或是直到下次系統重新開機。



警告
這是個重大安全事件。我們建議您盡量縮短停用即時防護的時間。如果您停用即時防護，您的電腦將暴露於各種惡意程式威脅之中。

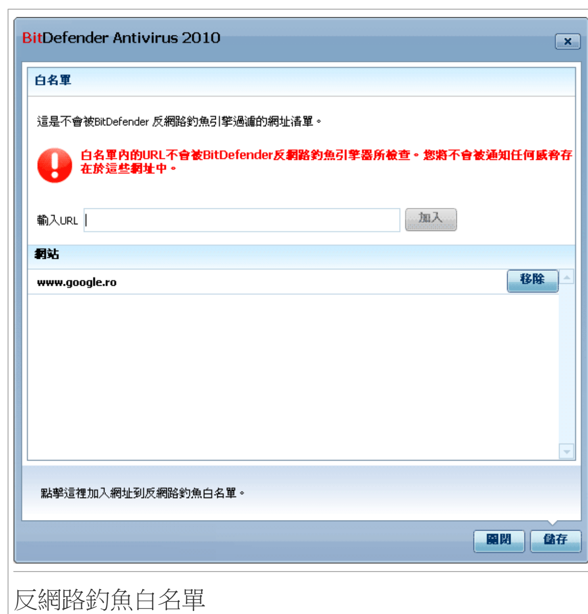
18.1.5. 設置反網路釣魚防護

BitDefender 為以下程式提供即時反網路釣魚防護：

- Internet Explorer
- Mozilla Firefox
- Yahoo 即時通
- Windows Live (MSN) Messenger

您可以針對特定或所有的應用程式停用反網路釣魚防護。

您可以點擊白名單以設置並管理不被BitDefender反網路釣魚引擎掃描的網站清單。



反網路釣魚白名單

您可以檢視所有不會被BitDefender反網路釣魚引擎掃描的網站。

要將網站加入白名單，在新的位址欄位輸入網站的網址並點擊加入。 白名單應該只包含您完全信任的網站。 舉例來說，加入您最近使用過的線上商店網站。



註

您可以利用BitDefender設立在瀏覽器的反網路釣魚工具列可以容易地管理防護工具，以及建立白名單。 更多詳細的資料，請參閱“整合入網頁瀏覽器” (p. 177)。

如果您想從白名單中移除網站，點擊對應的移除鈕。

點擊 儲存以儲存變更並關閉視窗。

18.2. 手動掃描進行中

BitDefender 的主要目的是維護您的電腦免受到病毒的威脅。保持新的病毒遠離您的電腦是最首要的目標，透過掃描電子郵件、新下載的檔案或複製到您系統的檔案。

在您安裝 BitDefender 前，可能已經有病毒存在於您的系統中。這是為什麼在您完成安裝 BitDefender 後，要求掃描您的系統，以找出存在的病毒。經常掃描您的電腦是個很好的建議。

在進階檢視點擊病毒防護>病毒掃描，可以設置與啟動手動掃描。



掃描任務

手動掃描是以掃描任務為基礎。掃描任務決定要被掃描的物件以及掃選項。 您可以用預設的掃描任務或是您(使用者)自訂的掃描任務來掃描電腦。您也可以規劃它們用基本的方式進行或是當您的電腦閒置時，以避免影響您的作業。

18.2.1. 掃描任務

在系統預設情況下BitDefender以幾項任務，建立包含一般的安全問題。 您也能建立您自訂的掃瞄任務。

每項任務有屬性允許您配置任務和看掃描結果的視窗。 對於更多信息，查看 “設定掃描任務” (p. 103).

掃描任務有三個類別：

- 系統任務 — 包含預設的系統掃描。下方是可用的掃描任務：

預設的任務	描述
深度系統掃描	掃描整個系統。 在預設的設置中，它能夠掃描您電腦中所有種類的惡意威脅。

預設的任務	描述
系統掃描	掃描整個系統，資料封存除外。 在預設的設定中，它將掃描除了後門程式之外的所有惡意程式類型。
快速的系統掃描	掃描Windows與Program Files資料夾。 在預設的設定中，可以掃描除後門程式外所有的惡意程式，但是不會掃描記憶體、登錄碼、cookies.
自動登入掃描	掃描使用者登入Windows就執行的項目。 自動登入掃描預設為停用的。 若您要使用此任務，按右鍵選擇排程，將任務設為於系統啟動時執行。 您可指定在系統啟動多久(分鐘)之後開始執行。



註

深度系統掃瞄 與 全系統掃瞄 是針對系統整體的分析任務，所以會需要較長的時間，我們建議您可以以低優先率執行此任務，甚至在您的系統閒置時更好。

- 用戶的任務 — 包含用戶定義的任務。

  有一個叫做 我的文件的掃描任務。 使用這個掃描任務執行掃描重要的使用者資料夾，如：我的文件 、桌面 以及 開始功能表。

- 其他的任務 — 包含其他掃描任務的清單。這些掃描任務參考到其他替代的掃描型態，而且它無法在這個視窗中執行。您只可以修改它們的設定及檢視掃描報告。

每個掃描任務的右邊有三個可按的按鈕：

- 排程任務 — 選擇將以排程來執行的任務。 從 屬性視窗裡，按下 排程器 頁面，您可以修改這個設定。
- 刪除 — 刪除所選擇的掃描任務。



註

系統掃描任務無法使用此功能。您不能刪除一個系統掃描任務。

- 立即掃描 — 執行所選的掃描任務，進行一個 立刻掃描。

在每個任務的左方您可看見屬性 — 允許您去設定任務以及檢視掃描日誌。

18.2.2. 使用捷徑選單

每個掃描任務都有一個捷徑選單可使用。在選擇的掃描任務按下滑鼠右鍵去開啟它：



捷徑選單

在捷徑選單上有以下可用的命令：

- 立即掃描 — 立刻掃描所選的掃描任務。
- 路徑 — 開啟 屬性 視窗路徑 標籤頁，您可以更改所選掃描任務的掃描目標。



註
在系統掃描任務頁面，這著選項將會顯示掃描路徑被替代，而只能看見掃描目標。

- 排程 — 選擇將要排程執行的任務。 從 屬性視窗裡，點擊 排程器 標籤，您可以在此進行任務排程。
- 檢視掃描日誌 — 開啟內容 視窗，掃描日誌 標籤頁，在掃描任務執行後，您可以檢視產生的報告。
- 複製任務 — 複製所選擇的任務。 當建立新的掃描任務時，您可以方便地修改已複製的掃描任務的設定。
- 刪除 — 刪除所選擇的掃描任務；



註
系統掃描任務無法使用此功能。您不能刪除一個系統掃描任務。

- 內容 — 開啟內容視窗，檢視 標籤頁，您可以更改所選掃描任務的設定=;



註
由於特性不同，在 其他任務 的類別裡，只有 內容 及 檢視掃描日誌 二種選項可使用。

18.2.3. 建立掃描任務

您可以選擇以下其中之一種方法建立掃描任務：

- 複製 一個存在的任務，您可以在 屬性 視窗中更改它的名稱或做必要的修改設定。
- 按下 新的任務 ，建立一個新的掃描任務並且設定它。

18.2.4. 設定掃描任務

每個掃描任務都有它的 屬性 視窗，您可以設定掃描的選項、掃描的目標、指定排程或檢視報告。從這個視窗裡的任務名稱按二下。下面的視窗將會出現： 點擊任務左邊的屬性鈕開啟視窗(或右鍵點擊任務並選取屬性)。



註
更多關於 日誌 頁面的資訊，請參考 "檢視掃描日誌" (p. 118)。

調整掃描設定

要調整任何特定的掃描任務，請按下滑鼠右鍵，並選擇屬性。 以下視窗將會顯示：



總覽

在這裡，您可以檢視掃描任務的資訊（名稱、上次執行的時間及排程狀態）及設定掃描的設定。

選擇掃瞄層級

首先，您必須選擇掃瞄的層級。拖曳滑桿到合適的掃瞄層級。

一共有三個掃瞄層級：

防護層級	描述
寬鬆	提供適當的偵測效率。耗用系統資源資源低。 只有應用程式被掃描是否有病毒。除了基本的特徵掃描，也使用了啟發式的分析。
預設	提供良好的偵測效率。耗用系統資源層級屬中等。 所有檔案都被掃描是否有病毒及間諜程式。除了基本的特徵掃描，也使用了啟發式的分析。
高	提供高水準的偵測效率。耗用系統資源層級較多。 所有檔案及封存檔都被掃描是否有病毒及間諜程式。除了基本的特徵掃描，也使用了啟發式的分析。

在掃描程序中可用到的一系列設定選項：

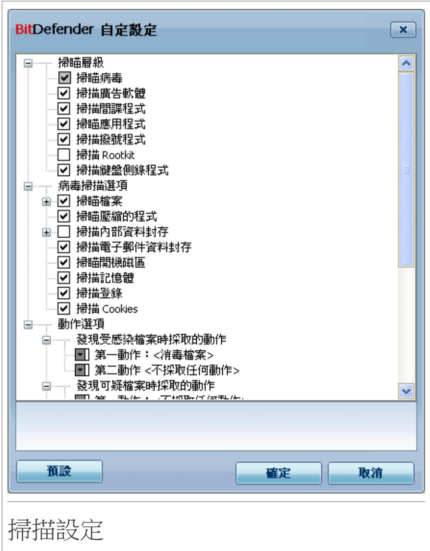
- 以低優先權執行任務. 降低掃描程序的優先權。您可以讓其他程式執行的更快，但這個掃描程序將會花更長的時間去完成。
- 將掃描視窗最小化到系統列. 將掃描視窗最小化到 系統工具列。可以按二下 BitDefender 圖示去開啟它。
- 當掃描完成時若沒有發現病毒，將這台電腦關機

按下 確定 要保存變動和關上視窗。 進行任務，點擊掃描 。

自訂掃瞄層級

進階的使用者可以使用 BitDefender 所提供的掃描設定。掃描器中可以設定指定特定的副檔名、目錄或您所知道無害的檔案。這將會減少掃描時間並加快您系統掃描的反應時間。

按下 自訂，將會出現一個新視窗，您可以設定自己的掃描選項：



掃描設定

掃描的選項以可擴展的選單方式呈現，非常相似於 Windows 檔案總管。 點擊 "+" 的小方框以展開選項或點擊 "-" 的小方框關閉選項。

掃描選項被分為三種類型：

● 掃瞄層級. 從掃瞄層級選單選擇適合的選項，指定您要BitDefender掃瞄的惡意程式類型。

選項	描述
掃描病毒	掃描已知病毒。 BitDefender也能夠偵測到不完整的病原體，因此能夠移除您系統內的可能威脅。
掃描廣告程式	掃描廣告程式威脅。被偵測到的檔案將被當成受感染的檔案。如果這個選項啟動時，包含廣告元件的軟體將無法運作。
掃描間諜程式	掃描已知的間諜程式。被偵測到的檔案將被當成受感染的檔案。
掃描應用程式	掃描可能會被利用為間諜工具的正當程式。
掃描撥號程式	掃描高收費陷阱的撥號程式。這些被掃描到的檔案將被當成受感染的檔案。如果這個選項啟動時，包含這類型撥號程式的軟體將無法運作。

選項	描述
掃描rootkits	掃描隱藏的物件，一般統稱rootkits。

● 病毒掃描選項． 指定要被掃描的物件類型 (資料封存、檔案、電子郵件，等) 以及其他選項。這個設定可以從 病毒掃描選項 中去進行設定。

選項		描述
掃描檔案	掃描所有檔案	所有被存取的檔案都將被掃描，不管其類型為何。
	只掃描應用程式檔案	只有程式檔案才會被掃描。這代表只有以下的副檔名將被掃描：exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml 及 nws。
	掃描使用者定義的副檔名	只有被使用者指定的副檔名將會被掃描。這些副檔名必須以"；" 做區隔。
掃描壓縮檔案		掃描壓縮的檔案。
掃描內部資料封存		掃描內部一般封存檔，例如.zip、.rar、.ace、.iso與其它。 點擊掃描安裝工具與chm資料封存的方塊，若您要掃描這些檔案。 掃描被封存的檔案會需要更多時間並需要較多的系統資源。 您可以在此輸入大小(KB)以限制掃描檔案封存的大小上線限制掃描檔案封存大小。
掃描內部電子郵件資料封存		掃描電子郵件資料封存。
掃描開機磁區		掃描系統開機磁區。
掃描記憶體		掃描記憶體是否有病毒或其他的惡意程式。
掃描登錄		掃描登錄內容。
掃描 Cookies		掃描 cookie。

● 動作選項． 指定要在每個檔案目錄所採取的動作。



註

要設置新的動作，點擊現在的第一個動作 並選取想要的選項。 設定第二個動作以在第一個動作失敗時執行。

- 選擇當偵測到受感染的檔案時執行的動作： 有以下選項可選：

動作	描述
沒有採取動作	在偵測到受感染的檔案時將不會有任何行動。這些檔案將會出現在報告裡。
消毒檔案	從受感染的檔案中移除惡意程式碼。
刪除檔案	立刻刪除受感染的檔案，不經任何警告。
移動檔案到隔離區	移動受感染的檔案到隔離區。 隔離的檔案無法被執行或開啟，如此可避免被感染的風險。

- 偵測到可疑檔案時所採取的行動。 有以下選項可選：

動作	描述
沒有採取動作	不會採取行動在可疑檔案。這些檔案將出現於報告檔案。
刪除檔案	立刻刪除受感染的檔案，不需任何警告。
移動檔案到隔離區	移動可疑的檔案到隔離區。 隔離的檔案無法被執行或開啟，如此可避免被感染的風險。



註

假如有檔案被探索式分析偵測為可疑的，我們建議您將這些檔案送交至BitDefender Lab。

- 選擇當偵測到隱藏的物件(後門程式)執行的動作。 有以下選項可選：

動作	描述
沒有採取動作	在偵測到隱藏檔案時將不會有任何行動。這些檔案將會出現在報告裡。
更改檔名	加入.bd.ren到隱藏的檔案名稱。 如此，您將能夠於您的電腦搜尋並找到(若有)這樣的檔案。
移動檔案到隔離區	移動隱藏檔案到隔離區。 隔離的檔案無法被執行或開啟，如此可避免被感染的風險。



註

請注意這些隱藏的檔案不是您刻意在系統上隱藏的檔案。這些檔案是被特別的程式或技術所隱藏的。 Rootkit本身並非惡意程式。它們常被用在病毒或間諜程式以避開防毒程式的偵測。

□密碼保護與加密檔案動作選項. 用Windows保護的檔案對您而言是重要的。 這是為什麼您可以設置不同的動作針對受感染的或可疑的受Windows加密檔案。 另外一個需要決定動作的是受密碼保護封存檔。 受密碼保護的檔案無法被掃描。 使用這些選項以設置處理加密檔案與封存檔的動作。

- 發現受感染的被加密檔案時採取的動作. 選擇發現Windows加密檔案受感染所要採取的動作。 有以下選項可選：

動作	描述
沒有採取動作	只會紀錄使用Windows加密的受感染檔案。 掃描完成後，您可以開啟掃描記錄檢視掃描結果。
消毒檔案	從受感染的檔案中移除惡意程式碼。 由時候消毒的動作會失敗，像是受感染的檔案在郵件封存內部的時候。
刪除檔案	立刻刪除受感染的檔案，不經任何警告。
移動檔案到隔離區	隔離區資料夾 隔離的檔案無法被執行或開啟，如此可避免被感染的風險。

- 發現可疑的被加密檔案時採取的動作. 選擇發現可疑的Windows加密檔案所要採取的動作。 有以下選項可選：

動作	描述
沒有採取動作	只會紀錄使用Windows加密的可疑檔案。 掃描完成後，您可以開啟掃描記錄檢視掃描結果。
刪除檔案	立刻刪除受感染的檔案，不需任何警告。
移動檔案到隔離區	移動可疑的檔案到隔離區。 隔離的檔案無法被執行或開啟，如此可避免被感染的風險。

- 當發現密碼保護的檔案時採取的動作. 選擇當偵測到受密碼保護的檔案時執行的動作。 有以下選項可選：

動作	描述
只有日誌	掃描記錄只保存記錄受密碼保護的檔案。 掃描完成後，您可以開啟掃描記錄檢視掃描結果。
詢問密碼	當偵測到受密碼保護的檔案時，詢問使用對應的密碼以掃描該檔案。

如果您按下 預設層級 您將載入預設的設定值。 按 確定 儲存這個設定並關閉視窗。

設定掃描目標

要設定特定使用者掃描任務的掃描選項，右鍵點擊任務並選取路徑。如果您已經開啟了任務的屬性視窗，選取路徑標籤。 以下視窗將會顯示：



掃描目標

您可以看見本機、網路、可拆除式磁碟中的檔案。所有被選擇的物件都會被掃描。

這個頁面包含了以下的按鈕：

- 新增資料夾 — 開啟一個瀏覽的視窗，您可以選擇所要掃描的檔案/資料夾。



註
您可以將檔案拖曳增加至檔案/目錄到清單中。

- ">移除物件 — 從掃描清單中移除先前所選擇的檔案或目錄。



註
只有後來被加入檔案 / 資料夾才能被刪除。

除了上面解釋過的按鈕，也有一些選項允許您快速選擇掃描位置。

- 本機磁碟 — 掃描本機磁碟。
- 網路磁碟 — 掃描所有網路磁碟。
- 可拆除式磁碟 — 掃描可拆除式的磁碟 (光碟、軟碟)。
- 所有項目 — 掃描所有磁碟，不管是本機、網路或者可拆除式的磁碟。



註
如果您想要掃描整個電腦是否有病毒，請選擇核取方塊對應的 所有項目。

按下 確定 要保存變動和關上視窗。 進行任務，點擊掃描 。

檢視系統任務的掃描目標

您無法變更在系統任務目錄下的掃描目標 您只可以看見掃描的目標。

若要檢視特定任務的掃描目標，按下滑鼠右鍵，並選擇顯示任務路徑。 以系統掃描為例，以下的視窗將會出現：



全系統掃描的掃描目標

系統掃描 與 深度系統掃描 將會掃描所有的本機磁碟，而 快速系統掃描只會掃描 Windows 與 Program Files 的檔案與資料夾。

點擊 確定 關閉視窗。 要執行本任務，按下 掃描。

排程掃描任務

在複雜的掃描任務中，掃描程序將花費一些時間，如果您可以關閉其他應用程式，那掃描工作將會進行得更順利。這也就是為什麼當您沒有使用電腦或者電腦閒置時，是您進行排程掃描的最佳時機。

要檢視特定任務的排程或修改它，右鍵點擊任務並選取排程。如果您已經在任務屬性視窗中，選取排程標籤。 以下視窗將會顯示：



排程器

您能見到排程任務，如果有的話。

當排程一個掃描任務時，您必須選擇以下選項的其中之一：

- 未被排程 — 只有當使用者要求時，這些任務才會被啟動。
- "一次 — 在一定的時間，只執行一次的掃描任務。在 開始日期/時間 欄位，指定開始的日期及時間。
- 週期性 — 週期地執行掃描任務，在一定的時間間隔(小時、天、週、月、年) 依指定的日期及時間開始進行掃描。

  在確定的時間間隔裡，如果您想要重覆某個掃描任務，請選擇 定期 並且編輯 每一欄位裡 minutes /hours /days / weeks/ months/ years 的數字，以指出掃描程序的執行頻率。您必須在 開始日期/時間 欄位上指出開始執行的日期及時間。
- 未被排程 — 只有當使用者要求時，這些任務才會被啟動。

按下 確定 要保存變動和關上視窗。 進行任務，點擊掃描 。

18.2.5. 正在掃描檔案與資料夾

在您開始一個掃描程序之前，您應該先確認BitDefender 的惡意程式驗證碼是最新的。 建議您使用最新的更新檔資料掃描您的電腦以獲得最完善的防護。 要確認上一次更新為何時，切換到進階檢視並到更新>更新標籤頁。



註
為了讓 BitDefender 完成一個完整的掃描，您必須關閉所有開啟的程式。特別是電子郵件程式(如：Outlook、Outlook Express 或 Eudora) 更需要在完整掃描時進行關閉。

掃描提示

您可在此找到一些有用的提示：

- 執行一個完整掃描所需的時間取決您硬碟的大小。 因此建議您可以於不需要用電腦的時間掃描您的系統。

  您可以排程掃描 在您方便的時間。 確認您的電腦正在運作。 若使用Windows Vista，請確認您的系統不是休眠狀態。

- 若您時常從網路下載檔案，您可以使用將資料夾設為掃描目標建立一個專門掃描這些檔案的任務。 將任務排程於您要的時間執行。
- 有一種病毒會變更Windows的設定在開機時自動地執行。 要防範這類的病毒，您可以使用登入掃描，在系統啟動時執行掃描。 請注意登入掃描可能會在啟動時影響您的系統效能。

掃描方式

BitDefender 提供四個型態的手動掃描：

- 立刻掃描 —從系統/用戶任務進行掃瞄任務。
- 右鍵選單掃描 — 在檔案或者目錄按下滑鼠右鍵，並選擇 用 BitDefender掃描。
- 拖放掃描 — 拖曳一個檔案或目錄放到 掃描活動列上。
- 手動選擇掃描 — 使用BitDefender 手動選擇掃描瀏覽並選擇要掃描的檔案或檔案。

立刻掃描

要掃描您的電腦或部分，您能進行預設的掃瞄任務或您自訂的掃瞄任務 這被稱為立刻掃描。

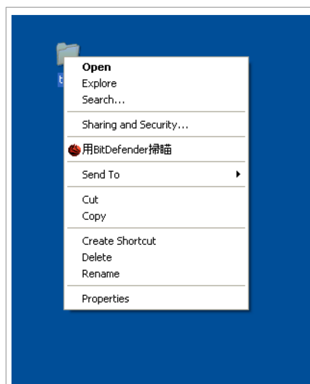
您可以選擇以下方式的其中之一：

- 在清單要執行的任務連續點擊兩下。
- 按下所對應任務的 立即掃描 鈕。
- 選擇任務，並按下執行任務。

病毒掃描精靈會出現並引導您完成整個掃瞄過程。

右鍵選單掃描

您可以直接使用右鍵選單直接掃描檔案或是資料夾。 右鍵選單掃描



右鍵選單掃瞄

在您想要掃描的檔案或目錄按下滑鼠右鍵，並選擇 用 BitDefender 掃描。 病毒掃描精靈會出現並引導您完成整個掃瞄過程。

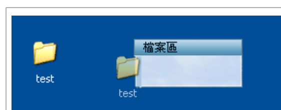
在 右鍵選單掃描 任務的 屬性 視窗，您可以修改掃描選項並檢視報告檔案。

拖放掃描

拖放您想要掃描的檔案或資料夾到下方顯示的 掃描活動列。



拖曳檔案



放開檔案

病毒掃描精靈會出現並引導您完成整個掃瞄過程。

手動選擇掃描

您能夠在開始功能表中的程式集使用手動選擇掃描選項，直接瀏覽並掃描檔案。



註

手動選擇掃描是一個很方便的功能，在Windows的安全模式中也能使用。

如果您想要在開始功能表執行BitDefender掃描功能，請依照Windows 開始程式集的路徑：開始 → 程式集 → BitDefender 2010 → BitDefender 手動選擇掃描。 以下視窗將會顯示：



手動選擇掃描

點擊 加入資料夾，選擇要掃描的位置並點擊 確定。 若要掃描多個資料夾，請重覆此動作。

您所選擇的位置將會出現在掃描目標欄位。 如果您要變更路徑，只要點擊旁邊的 移除鈕。 點擊移除全部路徑鈕以移除所有加入清單的位置。

當您選好位置，點擊繼續。 病毒掃描精靈會出現並引導您完成整個掃瞄過程。

病毒掃描精靈

當您執行手動掃描，掃描精靈將會出現。 依照三步驟指引執行掃描任務。



註

若掃描精靈沒有出現，則此任務可能被設為在背景作業。 您可以在系統工具列看見 掃描程序圖示。 您可以點擊此圖示開啟掃描視窗並檢視掃描程序。

步驟 1/3 — 進行掃描

BitDefender 將會開始掃描選擇的項目。



掃瞄中

您能見到掃描狀態和統計（掃描速度，使用時間，掃描 / 受傳染的 / 可疑的 / 隱藏的物件和其他的數目）。

等待BitDefender 完成掃描。



註
掃描程序將依它的複雜程度而需花費一些時間。

密碼保護的封存檔. BitDefender 在掃描過程偵測到一個密碼保護的封存檔，預設的動作是詢問密碼，您會被詢問要提供密碼。 受密碼保護的檔案無法被掃描。 有以下選項可選：

- 密碼. 若您要BitDefender掃描封存檔，點選此選項並鍵入密碼。 若您不知道密碼，選擇其他選項。
- 不要詢問密碼並跳過此物件. 選擇此選項跳過掃描封存檔。
- 跳過所有受密碼保護的物件不要掃描。. 選擇此項目若您要不被詢問任何密碼保護的項目。 BitDefender 將不會掃描它們但會紀錄在掃描日誌檔案。

點擊 確定以繼續掃描。

停止或暫停掃描. 您可以點擊停止，完全停止掃描程序，而您將會直接被引導到最後的步驟。 您可以點擊暫停，暫時停止掃描程序。點擊 回復以繼續掃描任務。

步驟 2/3 — 選擇動作。

當掃描程序完成，一個新的視窗會出現，您可以在該視窗檢視掃描結果。



動作

您可以檢視可能影響您的系統的事件數量。

被感染的物件會依照感染它們的惡意程式分組做表示。 點擊對應的威脅，您便可以得到更多關於被感染物件的資訊。

您可以針對不同的威脅類型的分組採取全體行動，也可以逐項地進行處理。

下列的選項會出現在選單中：

動作	描述
沒有採取動作	不對偵測到的檔案採取任何行動。 掃描完成後，您可以開啟掃描記錄檢視掃描結果。
消毒檔案	從受感染的檔案中移除惡意程式碼。
刪除檔案	刪除所有被偵測的檔案
移到隔離區	移動偵測到的檔案到隔離區。 隔離的檔案無法被執行或開啟，如此可避免被感染的風險。

動作	描述
更改檔名	加入.bd.ren到隱藏的檔案名稱。 如此，您將能夠於您的電腦搜尋並找到(若有)這樣的檔案。 請注意這些隱藏的檔案不是您刻意在系統上隱藏的檔案。這些檔案是被特別的程式或技術所隱藏的。 Rootkit本身並非惡意程式。它們常被用在病毒或間諜程式以避開防毒程式的偵測。

點擊 繼續 以套用指定的動作。

步驟 3/3 — 檢視結果

當BitDefender 完成修復動作，將會出現一個掃描結果的視窗。

BitDefender Antivirus 2010 - 我的文件

步驟1

結果	
已解決項目：	1
未解決的項目：	0
受密碼保護的項目：	0
過度壓縮的項目：	0
略過的項目：	0
失敗的項目：	0

1個威脅已被移除。

病毒掃描已完成。這些是此掃描任務的統計資料。

bitdefender 檢視記錄 關閉

摘要

您可以檢視結果。 若您要了解詳細的掃描資訊，點擊顯示日誌檔案來檢視掃描日誌。



重要
您的系統可能被要求重新啟動以完成您的清理程序。

按下 關閉 關閉視窗。

BitDefender 可能無法解決某些問題

在大部分的情形中，BitDefender 能夠成功地消毒被感染的檔案或是將之隔離。 然而，可能有極少部分的問題無法被解決。

在這種情況下，我們建議您聯絡BitDefender 在網頁www.bitdefender.com的支援團隊。 我們的技術支援代表將會協助您解決您遭遇的問題。

BitDefender 偵測到可疑的檔案

可疑的檔案是被探索式分析歸類被潛在的、沒有正式發布惡意程式碼所感染的檔案。

如果偵測到可疑的檔案，您會被要求將可疑的檔案遞交給BitDefender Lab。 點擊好將這些檔案送交BitDefender Lab做進一步的分析。

18.2.6. 檢視掃描日誌

當任務結束時，在任務按下滑鼠右鍵並選擇日誌，您可以檢視掃描結果。 以下視窗將會顯示：



掃瞄記錄

在此您可以檢視被執行過的任務報告。 在這裡您可以看到掃描任務被執行時，每一個時間所產生的報告檔案。當掃描被執行及掃描任務完成時，每個檔案會包含它的詳細資訊，清除/受感染、日期及時間等訊息。

有二個按鈕是可用的：

- 刪除日誌 — 刪除選擇的掃瞄日誌；
- 顯示日誌 — 檢視選擇的掃描日誌； 掃描報告將用您的預設瀏覽器開啟。

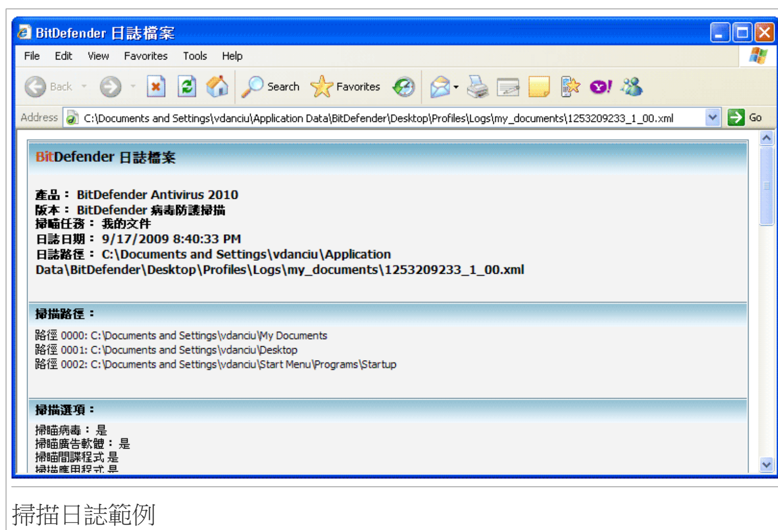


註
在檔案上按下右鍵也可以執行檢視/刪除的動作。

按下 確定 要保存變動和關上視窗。 進行任務，點擊掃描 。

掃描日誌範例

下列表呈現一個掃描日誌的範例：



掃描日誌範例

掃描日誌包含了詳細的資訊，例如：掃描項目、掃描目標、發現的威脅與所採取的行動。

18.3. 被掃瞄排除的物件

當您可能需要掃描時，某些檔案會被排除。 例如，您可以要EICAR存取測試掃描或 .avi 檔案在要求時掃描。

BitDefender 允許您排除物件不被掃描，如此可以減少掃描所花費的時間以及減少對您工作的影響。

兩種能夠被排除掃描的物件：

- 路徑 — 排除掃描所有在指定路徑下的檔案與資料夾。
- 副檔名 — 排除掃描所有特定副檔名的檔案。



註

所有被自動掃描排除的物件將不會被掃描，無論您是否有執行。

要管理被排除掃描的物件，請在進階檢視病毒防護>例外。



指定例外

您可看見被排除掃描的物件。在每個物件上您可以看見它是被哪一種掃描類型排除。



註

這裡被指定的例外將無法使用右鍵選單掃描。 右鍵選單掃描屬於手動掃描的一種：您可以在要掃描的檔案或資料夾點右鍵並選擇用BitDefender掃描。

要移除項目，選擇並點擊 刪除鈕。

要編輯項目，只需選擇並點擊 編輯 按鈕或者連續按二下。 一個新的視窗將會出現，您可以在此編輯要被掃描排除的副檔名或是路徑，您也可以在此設定需要排除的掃描類型。編輯完成後，請點擊確定。



註

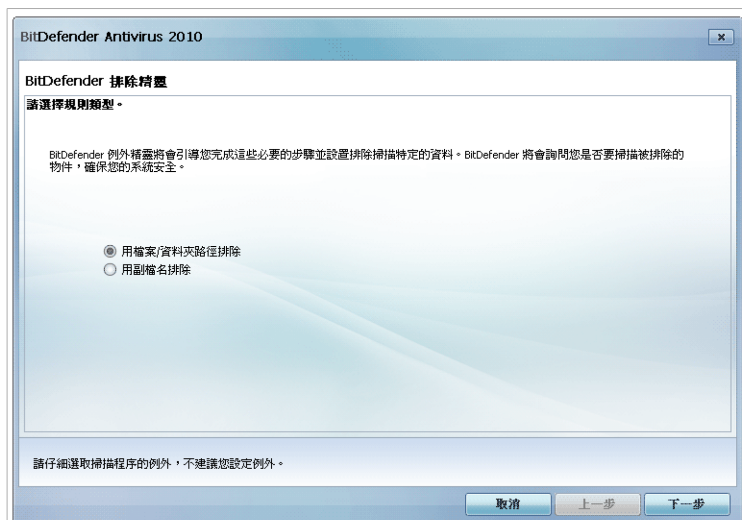
您也可以在物件上按下右鍵，使用右鍵功能表編輯。

在您尚未按下套用之前，可點擊 放棄 ，回復尚未儲存的設定。

18.3.1. 排除掃描路徑

要排除捷徑掃描的路徑，點擊 加入 按鈕. 一個設置精靈將會出現，並且引導您完成設定

步驟 1/4 — 選擇物件類型



物件類型

選擇要被排除的路徑選項

點擊 下一步。

步驟 2/4 — 指定要排除的路徑



排除的路徑

您可依照下列方式設定：

- 按下 瀏覽，選擇要排除的檔案或資料夾並按下 加入。
- 鍵入您要排除的路徑並點擊加入。



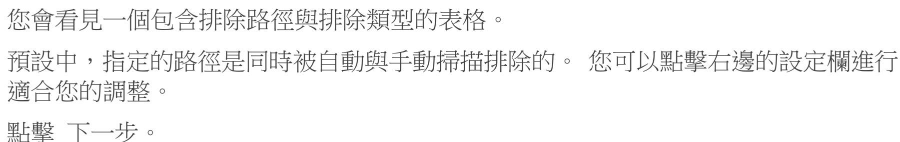
註
假如指定的路徑不存在或是出現錯誤訊息，點擊確定並檢查路徑的正確性。

當您加入路徑時，它會出現在表格中。

要移除項目，選擇並點擊 刪除鈕。

點擊 下一步。

步驟 3/4 — 選擇掃描類型



掃描類型

您會看見一個包含排除路徑與排除類型的表格。

預設中，指定的路徑是同時被自動與手動掃描排除的。 您可以點擊右邊的設定欄進行適合您的調整。

點擊 下一步。

步驟 4/4 — 掃描被排除的檔案



掃描被排除的檔案

強烈建議您掃描在指定路徑的檔案以確認它們沒有受到感染。 選擇此方塊在它們被排除之前先進行掃描。

點擊 完成。

18.3.2. 排除掃描的副檔名

要排除副檔名，請按下 加入 按鈕。 一個設置精靈將會出現，並且引導您完成設定。

步驟 1/4 — 選擇物件類型

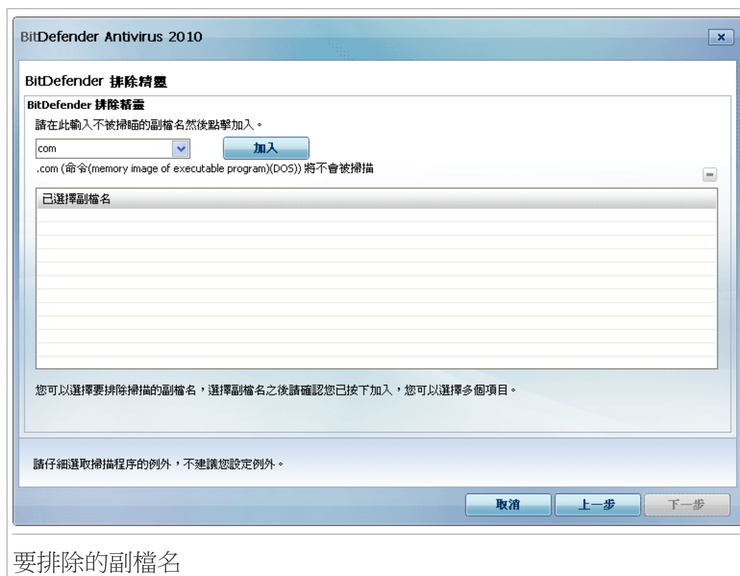


物件類型

選擇要排除的副檔名選項。

點擊 下一步。

步驟 2/4 — 指定的要排除的副檔名



要排除的副檔名

您可依照下列引導執行設定：

●從選單中選擇要排除的副檔名並且按下加入。



註
選單包含您系統所有副檔名的清單。當您選擇任何一個副檔名，您可以看見簡述(若有)。

●在編輯欄內鍵入您想排除的副檔名，並點擊加入。

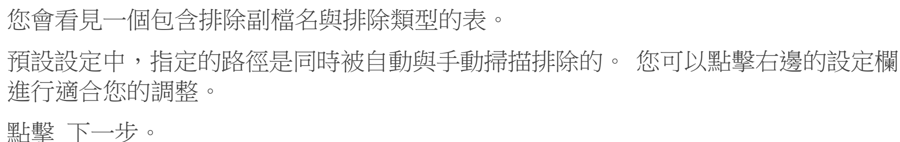
當您加入副檔名時，它會出現在表格內。

要移除項目，選擇並點擊 刪除鈕。

點擊 下一步。

步驟 3/4 — 選擇掃描類型

掃描類型

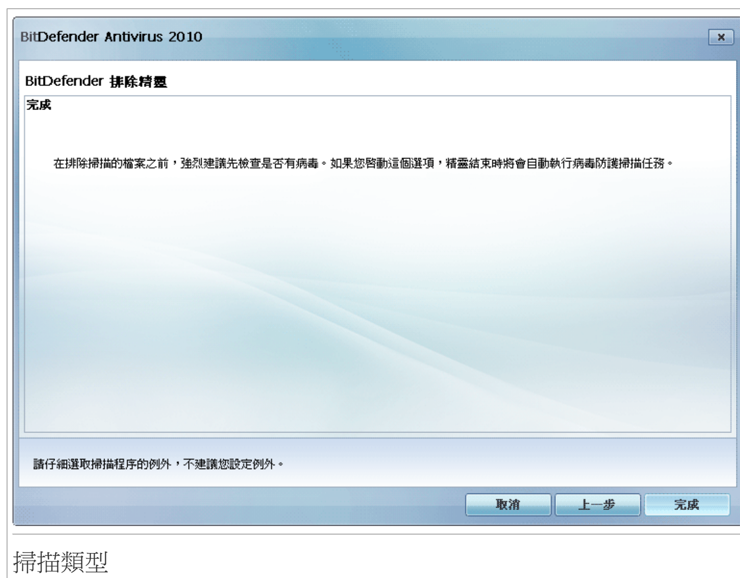


您會看見一個包含排除副檔名與排除類型的表。

預設設定中，指定的路徑是同時被自動與手動掃描排除的。 您可以點擊右邊的設定欄進行適合您的調整。

點擊 下一步。

步驟 4/4 — 選擇掃描類型



掃描類型

強烈建議您掃描指定副檔名的檔案以確認它們沒有受到感染。

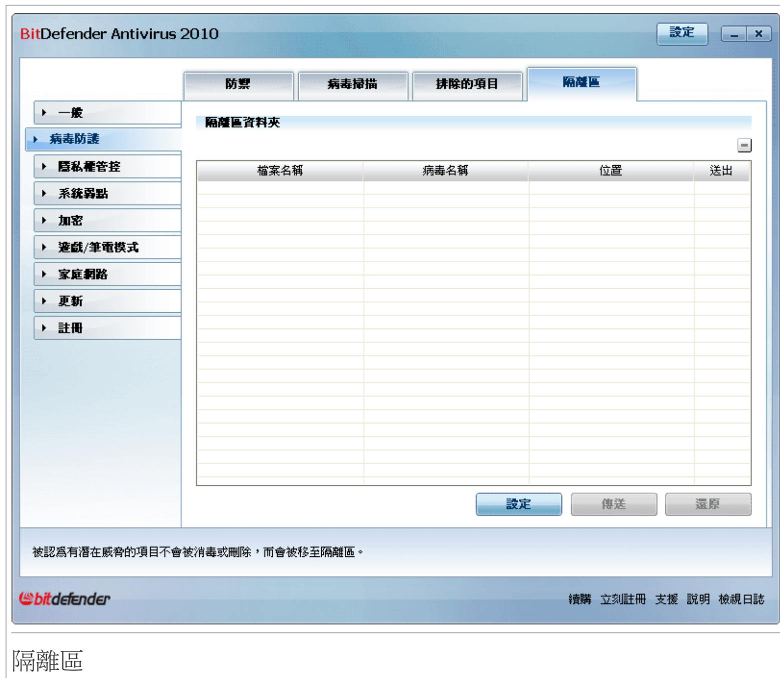
點擊 完成。

18.4. 隔離區

BitDefender 允許隔離受感染或可疑檔案到一個被防護的區域，名為隔離區。將這些檔案隔離在隔離區裡，會減少感染擴散的風險，同時，您也可以寄送這些檔案到 BitDefender lab。

此外，每次病毒碼更新完成後，BitDefender 會掃描被隔離的檔案。 已無害的檔案會自動被還原到原來的路徑。

在進階檢視點擊病毒防護>隔離區，便能調整設定並管理被隔離的檔案。



隔離區

隔離區頁面顯示目前所有被隔離的檔案。 每個被隔離的檔案您可以看見它的檔名、被偵測到的病毒、原始的檔案路徑、被隔離的日期及遞交的日期



註
當病毒在隔離區中，它不能造成任何的危害，因為它們無法被執行或讀取。

18.4.1. 管理被隔離的檔案

從隔離區，您可以寄送任何選擇的檔案到 BitDefender 實驗室，按下 寄送。BitDefender 預設每60分鐘自動遞交被隔離的檔案。

從隔離區選擇要刪除的檔案，點擊 刪除 鈕。如果您想要還原所選擇的檔案到它原始的位置，請按下 還原。

右鍵選單. 右鍵選單能夠讓您容易地管理隔離區。您可以選擇重新整理 更新隔離區內的項目。

18.4.2. 隔離區設定

要調整隔離區設定，按下 設定。 將會開啟一個新的視窗。



隔離區設定

您可以直接設定BitDefender執行下列動作：

刪除舊的檔案。． 要自動刪除舊的被隔離檔案，請選擇對應的選項。 您必須設定要刪除幾天以前被隔離的檔案，以及BitDefender 檢查舊檔案的頻率。



註
預設BitDefender會每天檢查一次並自動刪除30天以前的舊檔案。

刪除重複檔案。． 要自動刪除重複的隔離區檔案，選取對應的選項。 您一定要指定兩次重複檔案檢查之間的時間。



註
BitDefender 預設每天檢查隔離區中重複的檔案。

自動遞交檔案。． 如果您要自動遞交被隔離的檔案，選取對應的選項。 您必須指定遞交檔案的頻率。



註
BitDefender 預設每60分鐘自動遞交被隔離的檔案。

更新之後掃描被隔離檔案． 如果您要自動在每次更新完成後掃描被隔離的檔案，請選取對應的項目。 點選還原無害的檔案，您可以自動地將已處理過的無害檔案還原到原始位置。

按 確定 儲存這個設定並關閉視窗。

19. 隱私權管控

BitDefender 監視您的系統中多處可能受間諜程式攻擊的熱點，並檢查您的系統和軟件的異動。這是有效封鎖木馬程式及其他駭客安裝的工具程式，駭客會試圖竊取您的個人資料（如：信用卡號碼等）並寄送出去。

19.1. 隱私權管控狀態

要設置隱私權管控以及檢視其活動，請在進階檢視中進入隱私權管控>狀態。



隱私權管控狀態

您可以看到隱私權管控是啟動或停用。 如果您想更改隱私權管控狀態，請選取或取消選取對應的方塊。



重要

為了防止資料遭竊並保護您的隱私，請持續保持啟動隱私權管控。

隱私權管控使用這些重要防護管控來保護您的電腦：

- 身分管控 - 根據您在 身分頁面建立的規則，對外的網頁(HTTP)及電子郵件(SMTP)傳輸都會被過濾，以保護您的機密資料。

- 登錄管控 - 當有程式進入開始功能表執行而嘗試修改登錄項目時，先徵求您的同意。
- Cookie管控 - 當一個新的網站嘗試設定一個 cookie時，先徵求您的同意。
- Script管控 - 當一個網站嘗試啟動一個script或其他內容時，先徵求您的同意。

在頁底您可以看到身分管控統計資料。

19.1.1. 設置防護層級

您可以選擇最適合您安全需求的防護層級。拖曳滑桿設定合適的防護層級。

有三種防護層級：

防護層級	描述
寬鬆	所有防護管控都已停用。
預設	只有身分管控已啟動。
侵略的	身分管控、登錄管控、Cookie 管控和Script 管控 已啟動。

您可以點擊自訂層級以自訂防護層級。 在出現的視窗中，選擇您要啟動的防護管控並點擊確定。

點擊預設層級，將滑桿拖曳至預設層級。

19.2. 身分管控

保持機密資料的安全是個重要的議題。在網際網路的發展下，資料竊盜技術也隨之進步，它利用一些新的方法來騙取人們提供個人私密的資料。

不管是您的電子郵件或您的信用卡號碼，當落入壞人的手中，絕對會造成您重大的損失：您會發現您的信箱被垃圾郵件所淹沒，或是您將會絕望的面對一個掏空的銀行帳號。

身分管控能夠保護您在線上時免於被竊取敏感的資料。 根據您所建立的規則，身分管控將會掃描從網頁、電子郵件或即時通訊中有沒有出現特定字串(例如：信用卡號碼)。如果掃描到特定字串，該網頁、電子郵件或即時通訊將會被阻擋。

您可以建立規則以保護您的所有個人隱私資料，例如手機號碼、電子郵件位置，亦或是銀行帳戶資訊。 提供多使用者服務，不同的Windows使用者帳戶可以設置自己的身分保護規則。 若您使用系統管理員帳號，您建立的的規則也會套用到其他在本電腦登入的Windows 使用者帳號。

為什麼要使用身分管控？

- 身分管控對於阻擋鍵盤記錄的間諜程式非常有效。 這種惡意程式會紀錄您的鍵盤打字記錄，並利用網路傳送給駭客。 駭客可以藉此得到您的敏感資訊，例如銀行帳戶號碼、密碼，並使用它得利。

只要您建立了恰當的身分防護規則，即使間諜程式成功避開病毒防護的檢查，仍無法以電子郵件、網頁或即時訊息的方式傳送被偷取的資料。

- 身分管控能保護您不受網路釣魚企圖。(企圖偷取您的個人資訊)。 最常見的網路釣魚使用假郵件，讓您進入假的網頁輸入個人資訊。

  例如，您可能收到一封聲稱來自銀行的郵件，要求您緊急更新您的銀行帳戶資訊。這封郵件給您一個網頁連結，並要求你輸入個人資料。 即使郵件與網頁看似正常，其實它們都是假的。 如果您點擊了郵件中的連結、並在網頁中輸入您的個人資料，您將揭露這些資訊給網路駭客。

  如果您已設置恰當的身分防護規則，您就無法遞交個人資訊(例如您的信用卡號)至一個您未定義成例外的網頁。

要設置身分管控，請在進階檢視中進入隱私權管控>身分。



身分管控

如果您想要使用身分管控，請依照以下步驟：

1. 選取啟動身分管控核取方塊。
2. 建立規則以保護您的敏感資料。　要了解更多資訊，請參考“建立身分管控規則” (p. 135)。

3. 如果有需要，在您所建立的規則中定義特定的例外。 要了解更多資訊，請參考“定義例外” (p. 138)。
4. 若您是系統管理者，您可以將自己排除於其他人設定的身分管控規則。

   要了解更多資訊，請參考“其他管理者定義的規則。” (p. 140)。

19.2.1. 建立身分管控規則

要建立身分保護規則，請點擊 加入鈕並依照設置精靈進行。

步驟 1/4 - 歡迎視窗



歡迎視窗

點擊 下一步。

步驟 2/4 - 設定規則類型及資料

BitDefender 身分規則精靈

規則名稱

規則種類 pin

規則資料

"john").

在此區域輸入規則名稱。如此您才能夠辨別身分管控的規則。

上一步 下一步 取消

設定規則類型及資料

您必須設定以下的參數：

- 規則名稱 — 在編輯欄位中輸入規則的名稱。
- 規則類型 — 選擇規則類型 (住址、姓名、信用卡號碼、身分證號碼等)。
- 規則資料 —在編輯欄位中輸入您想要保護的資料。 舉例來說，如果您想保護您的信用卡號碼，在這裡輸入全部或部分的號碼。



註

如果您輸入少於三個字元，您將會被提示驗證資料。我們建議您最少三個字元以避免被阻擋錯誤發生。

在這裡您所輸入的資料都會被加密。為了加強安全性，請不要輸入完整的資料。

點擊 下一步。

步驟 3/4 - 選擇傳輸類型與使用者



選擇傳輸類型與使用者

選擇您希望BitDefender掃描的傳輸方式： 有以下選項可選：

- 掃描 HTTP — 掃描 HTTP(網站) 傳輸，並阻擋符合規則的外送資料。
- 掃描 SMTP — 掃描 SMTP(電子郵件) 傳輸，並封鎖符合規則的外送電子郵件。
- 掃描即時通訊 — 掃描即時通訊傳輸，並封鎖符合規則的外送即時訊息。

您可以選擇在整個單字符合規則資料時套用規則，偵測到的字串事件相符時套用規則。

指定規則套用的使用者。

- 只有我(目前的使用者) - 規則將只會套用到您的使用者帳戶。
- 有限的使用者帳戶 - 規則將會套用到您與有限的使用者帳號。
- 所有使用者 - 規則將會到用到所有Windows帳號。

點擊 下一步。

步驟 4/4 - 規則描述

規則描述

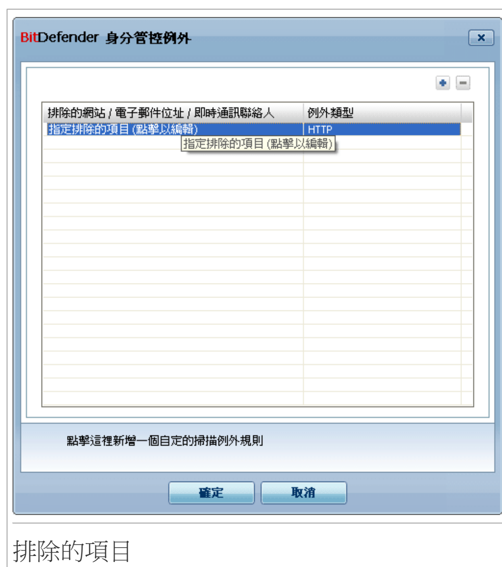
在編輯的欄位上輸入一個規則的簡短描述。 由於存取規則時，被阻擋的資料(字串)不會顯示，所以述能幫助您分辨規則。

點擊 完成。 規則將出現在表中。

19.2.2. 定義例外

這是您可能須要對特定的身分規則定義例外的情況。 當您真的需要將您的信用卡資料藉由網路傳送遞交時，您可以設定規則的例外。

要管理例外規則，按下 例外。



排除的項目

要加入例外，請依照下列步驟：

1. 點擊 加入按鈕以在表上新增項目。
2. 點擊兩下指定排除的項目，輸入您要加入例外的網址、電子郵件位址或即時通訊連絡人。
3. 點擊兩下傳輸類型並從選單選擇對應的您輸入的資料選項。
   - 如果您指定了一個網址，請選擇HTTP。
   - 假如您指定了一個電子郵件位址，請選擇SMTP。
   - 如果您指定了一個即時通訊連絡人，請選擇即時通訊。

要移除項目，選擇並點擊 移除鈕。

點擊確定 去儲存變更。

19.2.3. 管理規則

您可以在表格中檢視目前已建立的規則清單。

要刪除一個規則，只需點選規則並點擊 刪除鈕。

要編輯一個規則，只需點選規則並按下 編輯按鈕或者雙擊規則。一個新的視窗即會出現。

編輯規則

您可以在這裡變更規則的名稱、描述及參數(種類、資料及掃描傳輸的方式)。點擊確定 儲存設定。

19.2.4. 其他管理者定義的規則。

當您不是系統唯一管理者時，其他人也可以建立它們自己的身分規則。 若您不要其他人建立的規則影響您的作業，您可以從這些規則將自己排除限制。

您可以身分管控規則表格看見其它使用者建立的規則。每個規則都會列出其建立的使用者。

要將您自己從規則中排除，選取表格中的規則並點擊 Delete刪除鈕。

19.3. 登錄管控

登錄鍵 在 Windows 作業系統是一個非常重要的部份。這是 Windows 放置設定、安裝的程式、使用者資訊等相關重要設定的地方。

登錄鍵 也被使用來定義哪個程式在Windows啟動時自動執行。當使用者重新啟動電腦時，病毒也常利用這個方式自動啟動。

登錄管控監控Windows 登錄鍵的變化 - 這是偵測木馬程式有效的方法。每當程式試著修改登錄鍵，以便在 Windows 啟動時被執行時，它將會先警告您。



登錄警示

您可以看到正試圖更改Windows登錄鍵的程式。

若您無法辨識此可疑的程式，點擊阻擋以避免其更改Windows登錄鍵。 或者點擊允許以允許其更改。

根據您的回應，將建立一個規則並列於規則表格中。 若此程式再次要求更改登錄鍵，將自動套用相同的行動。



註
當您安裝新的程式且必須在下次系統啟動時執行，BitDefender將會提示您。多數情形下，這些程式是合法且可被信任的。

要設置登錄管控，請在進階檢視中進入隱私權管控>登錄。



登錄管控

您可以在表格中檢視目前已建立的規則清單。

要刪除一個規則，只需點選規則並點擊 刪除鈕。

19.4. Cookie管控

Cookies 是網際網路上一個常見的記錄。它是存在您電腦裡非常小的一些檔案。網站透過建立這些 cookies 以保持您的追蹤資訊。

Cookie 讓您的生活變得更方便。舉例來說，它們可以讓網站記住您的名字及相關的資訊，所以，您不需要每次造訪網站時都重新輸入這些資訊。

但透過追蹤您的記錄樣本，cookies也可能被利用洩露您的隱私資料。

Cookie管控能夠幫助您，在您啟動 Cookie管控時，新的網站試圖設定一個cookie將先徵求您的同意：



Cookie 警示

您可以看見正試圖寄送cookie檔案的應用程式名稱。

點擊是或否然後一個規則將會被建立、套用並列於規則表格中。

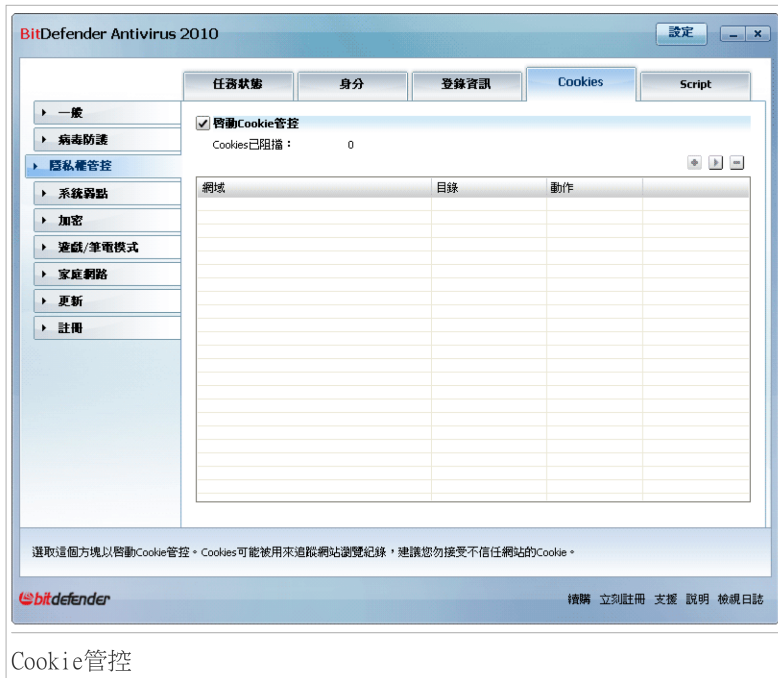
這將協助您選擇哪個網站您要信任或不信任。



註

現今大量的 cookie 被使用在網際網路上，Cookie 管控 一開始使用可能有點麻煩。首先，當網站試圖儲存 cookie 在您的電腦時，它將詢問一些問題。很快地，您新增常造訪的網站到規則清單裡，它將變得比以前更容易。

要設置Cookie管控，請在進階檢視中進入 隱私權管控>Cookie。



Cookie管控

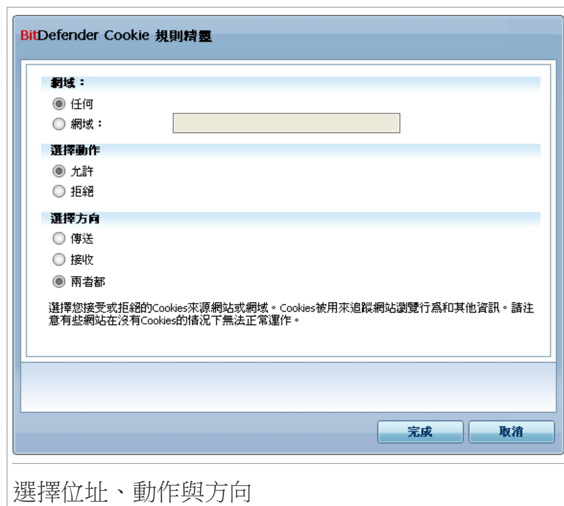
您可以在表格中檢視目前已建立的規則清單。

要刪除一個規則，只需點選規則並點擊 刪除鈕。 要變更規則參數，選擇規則並點擊 編輯 鈕，並在設置視窗中更改規則。

要手動增加規則，點擊 加入鈕並在視窗中設置規則參數。

19.4.1. 設置視窗

當您編輯或手動加入一個規則時，設置視窗將出現。



選擇位址、動作與方向

您可以設置參數：

- 網域位址 - 在規則裡，輸入所應套用的網域。
- 動作 - 選擇規則所要執行的動作。

動作	描述
允許	在這個網域的 cookie 將會被執行。
拒絕	在這個網域的 cookie 將不會被執行。

- 方向 - 選擇傳輸的方向。

類型	描述
外傳	這個規則只套用在傳回連線網站的cookies。
接收	這個規則只套用在從連線網站所接收的cookies。
兩者皆是	這個規則套用到進出二個方向。



註

您可以接受cookies但不回傳它們：拒絕　外送 方向。

點擊 完成。

19.5. Script管控

Scripts 及其他類似 ActiveX 管控 及 Java applets，是被用來建立互動式網頁，可以被設計成有害的程式。舉例來說，ActiveX 元素可以獲取您的資料，它們可以從您的電腦讀取資料、刪除資訊、擷取密碼並在您上線時攔截訊息。您應該只接受您所信任網站的主動式內容。

BitDefender 讓您選擇去執行這些元件或者封鎖它們的執行。

透過 Script 管控 您可以指定哪個網站是您信任或者不信任。BitDefender 將會先徵求您的同意無論何時一個網站試著啟動一個 script 或其他主動式的內容：



Script 警示

您可以檢視資源的名稱。

點擊是或否然後一個規則將會被建立、套用並列於規則表格中。

要設置Script管控，請在進階檢視中進入隱私權管控>Script。



Script管控

您可以在表格中檢視目前已建立的規則清單。

要刪除一個規則，只需點選規則並點擊 刪除鈕。 要變更規則參數，選擇規則並點擊 編輯 鈕，並在設置視窗中更改規則。

要手動增加規則，點擊 加入鈕並在視窗中設置規則參數。

19.5.1. 設置視窗

當您編輯或手動加入一個規則時，設置視窗將出現。



選擇位址與動作

您可以設置參數：

- 網域位址 - 在規則裡，輸入所應套用的網域。
- 動作 - 選擇規則所要執行的動作。

動作	描述
允許	在這個網域的 scripts 將會被執行。
拒絕	在這個網域的 scripts 將不會被執行。

點擊 完成。

20. 系統弱點

定期更新您所使用的作業系統以及重要應用程式，是保護您的電腦免於惡意程式威脅的重要步驟。　　此外，為了防止未經認可的來源存取您的電腦，您必須為您的每個 Windows 帳號設置安全的密碼。

BitDefender 會定期的檢查您的系統弱點並通知您存在的事件。

20.1. 任務狀態

要設置自動系統弱點檢查或執行系統弱點檢查，請在進階檢視選擇系統弱點>狀態。

事件	任務狀態	動作
重要的Microsoft更新	過期的	安裝
其他Microsoft更新	過期的	安裝
自動更新狀態	已啟動	無
Yahoo! Messenger	過期的	更多資訊
Firefox	過期的	更多資訊
Windows Live Messenger	過期的	更多資訊
amirea	危險的密碼	修復

系統弱點狀態

這表格顯示前一次弱點檢查的結果以及狀態。 您能檢視每個用來修復弱點的動作，如果有的話。 若動作為無，則該事件不會成為系統弱點。



重要

要自動通知您的系統或應用程式弱點，請保持 自動系統弱點檢查 啟動。

20.1.1. 正在修復系統弱點

取決於事件的種類，修復某一個系統弱點以下列所示進行：

- 若有可用的Windows更新，點擊在動作欄位的 安裝以安裝更新。
- 若應用程式未更新，請使用首頁連結以更新到最新版本。
- Windows帳戶的密碼有危險性，點擊修復 強制使用者於下次登入時變更密碼，或自行變更。 使用大小寫混用、數字或特殊符號 (例如#、$或@)，以加強密碼。

您可點擊立刻檢查並依照精靈的步驟進行弱點修復。 要了解更多資訊，請參閱 “系統弱點檢查精靈” (p. 56)。

20.2. 設定

要設置自動系統弱點檢查，請在進階檢視選擇系統弱點>設定。



自動系統弱點檢查設定

選取對應的核取方塊以指定您想要定期檢查的系統弱點。

- 重大Windows更新
- 定期Windows更新
- 應用程式更新

- 在 危險的密碼



註

如果您沒有選取系統弱點對應的核取方塊，BitDefender 將不再通知您相關的事件。

21. 即時通訊加密

BitDefender加密所有您的即時交談訊息，預設規定：

- 您的交談對象已安裝了支援即時通訊加密的BitDefender版本，並且即時通訊加密在您的即時通訊程式上已經啟動。
- 您和您的交談對象使用Yahoo即時通或是Windows Live (MSN) Messenger交談。



重要

若您的交談對象使用，如Meebo、或其他支援Yahoo即時通與Windows Live (MSN)的網頁型式聊天程式，BitDefender將無法加密對話。

要設置即時通訊加密，請在進階檢視中進入加密>即時通訊加密。



註

您可以從交談視窗中使用BitDefender工具列，輕易的設置即時通訊加密。 要了解更多資訊，請參閱“整合即時通訊程式” (p. 179)。



即時通訊加密

預設即時通訊加密同時在Yahoo 即時通和Windows Live (MSN) Messenger 上啟動。您可以選擇在特定的或所有的即時通訊程式上停用即時通訊加密。

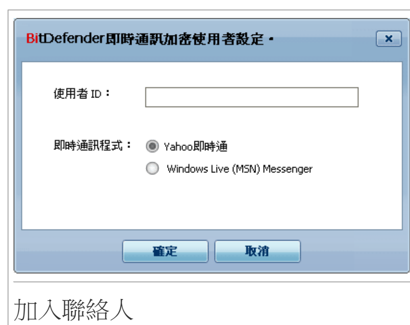
顯示兩份表格：

- 加密例外－停用加密的使用者帳號和對應的即時通訊程式。 要從清單上移除聯絡人，選取並點擊 移除鈕。
- 目前的連線 －目前使用中的即時通訊軟體及對應的聯絡人清單，以及它們是否啟動加密。 連線有以下幾個可能沒有被加密：
  - 您在對應的連線上已停用加密。
  - 您的連絡人沒有安裝支援即時通訊加密的BitDefender 版本。

21.1. 對特定的使用者停用加密

要對特定的使用者停用加密，請依照以下步驟：

1. 點擊 加入鈕以開啟設置視窗。



加入聯絡人

2. 在編輯欄位輸入聯絡人的使用者名稱。
3. 選取聯絡人對應的即時通訊程式。
4. 按下確定。

22. 遊戲/筆電模式

遊戲/筆電模組允許您設置特別的BitDefender 運行模式。

- 遊戲模式能夠暫時地變更防護設定，將系統運行的影響減至最低。
- 筆電模式能夠在您的筆電使用電池為電源時停用排定要執行的任務，以節省電池電力。

22.1. 遊戲模式

遊戲模式能夠暫時地變更防護設定，將系統運行的影響減至最低。　當您啟動遊戲模式，下列設定將會被套用：

- BitDefender警示及彈出示提示已全部停用。
- BitDefender 即時防護層級設定在 寬鬆e。
- 預設為不執行更新。



註

要變更設定，請至更新>設定 並取消選取 開啟遊戲模式時不要更新。

- 預設為停用排定的掃描任務。

預設BitDefender 會在您所設定的遊戲或全螢幕應用程式啟動時自動開啟遊戲模式。您可以手動進入遊戲模式，鍵入熱鍵Ctrl+Alt+Shift+G。 強烈建議您離開遊戲後關閉遊戲模式，您可以使用相同的熱鍵Ctrl+Alt+Shift+G以離開



註

當遊戲模式啟動時，您可以看見英文字母G顯示在 BitDefender圖示上。

要設置筆電模式，請在進階檢視選擇遊戲>筆電模式。



遊戲模式

您可以在此頁面的最上方檢視遊戲模式狀態。 您可以點擊進入遊戲模式或離開遊戲模式以變更目前狀態。

22.1.1. 設置自動遊戲模式

自動遊戲模式允許BitDefender 在偵測到執行遊戲時，自動進入遊戲模式。 您可以設置以下選項：

- 使用BitDefender提供的遊戲清單－以允許BitDefender 在偵測到正在執行清單上的遊戲時，自動進入遊戲模式。 要檢視清單，點擊管理遊戲然後點擊遊戲清單。
- 當切換至全螢幕時進入遊戲模式－當您使用的應用程式進入全螢幕時，自動切換至遊戲模式。
- 加入應用程式至遊戲清單？－在離開使用全螢幕的應用程式時，提醒是否加入遊戲清單。 如果將一個新的應用程式加入遊戲清單，下次您執行這個程式時將會自動進入遊戲模式。



註
如果您不想要BitDefender自動進入遊戲模式，請取消選取自動遊戲模式核取方塊。

22.1.2. 管理遊戲清單

在您執行遊戲清單上的應用程式時，BitDefender 將自動進入遊戲模式。 要檢視並管理遊戲清單，點擊管理遊戲。 將會開啟一個新的視窗。



遊戲清單

當這些時候新的應用程式將自動加入清單：

- 您開啟了一個BitDefender已知的遊戲。 要檢視清單，點擊遊戲清單。
- 在離開使用全螢幕的應用程式時，您在提醒視窗將它加入了遊戲清單。

如果您想要針對某個應用程式停用自動遊戲模式，請取消選取對應的核取方塊。 您應該針對某些時常使用全螢幕的應用程式停用自動遊戲模式，如瀏覽器或影音播放器。

要管理遊戲清單，您可以使用表格上方的按鈕。

- 加入以加入新的程式至遊戲清單。
- 移除 — 從遊戲清單中移除應用程式。
- 編輯 - 編輯已存在的遊戲清單。

加入或編輯遊戲

如果您加入或編輯了遊戲清單，將會出現以下視窗：



加入遊戲

點擊瀏覽以選取應用程式或在編輯欄位中輸入應用程式的完整路徑。

如果您不想在選定的應用程式執行時自動進入遊戲模式，點擊停用。

點擊確定以新增程式至遊戲清單。

22.1.3. 設置遊戲模式設定

要設置停止哪些排定的任務，選取這些選項：

- 啟動這個模組以修改掃描任務日程 - 當執行遊戲模式時，停止排程掃描任務。 您可以選擇以下選項的其中之一：

選項	描述
跳過任務	不要執行排定的任務。
延緩任務	在您離開遊戲模式後立刻執行排定的任務。

22.1.4. 變更遊戲模式熱鍵

您可以手動進入遊戲模式，鍵入熱鍵Ctrl+Alt+Shift+G。 如您想更改快速鍵，請按照以下步驟：

1. 點擊進階設定。 將會開啟一個新的視窗。



進階設定

2. 在使用熱鍵選項，設定您要的熱鍵：

- 您可以按下：Ctrl鍵(Ctrl)、Shift鍵(Shift)、Alt鍵(Alt)以選擇使用它們當做熱鍵。
- 在編輯欄鍵入字母以對應熱鍵。

舉例而言，如果您想要用Ctrl+Alt+D當作熱鍵，您必須按下Ctrl與Alt並且輸入D。



註
取消使用熱鍵旁的核取標記將停用熱鍵。

3. 點擊確定 去儲存變更。

22.2. 筆電模式

筆電模式特別為筆電的使用者設計，將可以在您使用電池為電源時，對筆電的電力消費影響達到最低。

在筆電模式中，排定的任務預設為不執行。

BitDefender 偵測到您的筆電使用電池為電源時，將自動進入筆電模式。 而BitDefender在偵測到您不再使用電池為電源時，將自動離開筆電模式。

要設置筆電模式，請在進階檢視選擇遊戲>筆電模式。



筆電模式

您可以檢視筆電模式是否啟動。 當使用筆電模式時，BitDefender 會套用使用電池時的設定。

22.2.1. 設置筆電模式設定

要設置停止哪些排定的任務，選取這些選項：

- 啟動這個模組以修改掃描任務日程 - 當執行筆電模式時，停止排程掃描任務。 您可以選擇以下選項的其中之一：

選項	描述
跳過任務	不要執行排定的任務。
延緩任務	在您離開筆電模式後立刻執行排定的任務。

23. 家庭網路

網路模組提供您管理每一台家庭電腦中安裝的BitDefender。



網路區域

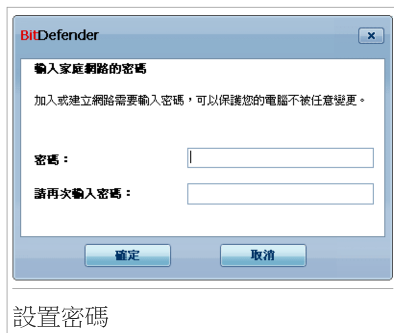
要管理您家庭電腦安裝的BitDefender，請您依照下列步驟：

1. 在您的電腦加入BitDefender家庭網路。 加入網路，為家庭網路管理設置一個管理者密碼。
2. 使用您想管理與加入網路的電腦，並設定密碼。
3. 回到您的電腦，並新增這些您想管理的電腦。

23.1. 加入BitDefender 網路

要加入BitDefender 家庭網路，請依照下列步驟：

1. 點擊啟動網路。 將提示您設置家庭管理密碼。



設置密碼

2. 在兩個文字框中輸入相同密碼。

3. 按下確定。

您可以在網路地圖上看到電腦名稱。

23.2. 加入電腦至BitDefender 網路

加入電腦至BitDefender 網路前，您必須先在每一台電腦設置BitDefender家庭管理密碼。

要加入電腦至BitDefender 網路，請依照下列步驟：

1. 點擊加入電腦。 將提示您輸入本地家庭管理密碼。



輸入密碼

2. 輸入家庭管理密碼，並點擊確定。 將會開啟一個新的視窗。



加入電腦

您可以檢視網路中的電腦清單。 小圖示的意義如下：

顯示一台線上電腦，但未安裝BitDefender。

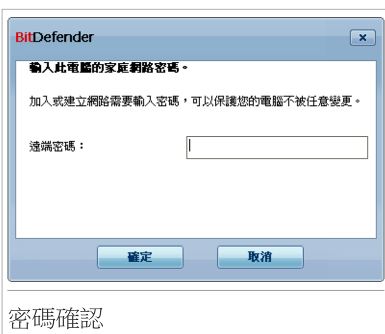
顯示一台線上電腦，已安裝BitDefender。

顯示一台離線電腦，已安裝BitDefender。

3. 您可以選擇以下動作：

- 從清單中選擇要加入的電腦名稱。
- 在對應欄位輸入要加入的電腦IP位置或電腦名稱。

4. 點擊加入。 將提示您輸入電腦的家庭管理密碼。



密碼確認

5. 輸入該電腦的家庭管理密碼。
6. 按下確定。 若密碼輸入正確，該電腦將出現在網路地圖上。



註
您最多可以加入五台電腦至網路地圖。

23.3. 管理BitDefender網路

只要您成功建立一個BitDefender家庭網路，您就可以管理所有電腦中的BitDefender。



網路區域

移動游標至網路地圖上的電腦，您可以查看該電腦的資訊概要(名稱、IP位置、系統安全事件數量、BitDefender註冊狀態)。

在網路地圖上的電腦名稱點擊右鍵，您可以查看所有能在遠端電腦上執行的管理任務。

● 從家庭網路移除電腦

讓您能夠從網路中移除電腦。

● 在這台電腦註冊BitDefender

讓您能夠以授權序號註冊BitDefender。

- 設置設定密碼於遠端電腦

  讓您能夠建立密碼以限制變更BitDefender的設定。

- 執行手動掃描任務

  讓您能夠在遠端電腦上執行手動掃描，您可以執行下列任務：我的文件掃描、系統掃描或深度系統掃描。

- 在這台電腦上修復所有事件

  讓您透過修復所有事件 精靈以修復可能影響您電腦安全的事件。

- 檢視歷史/事件

  讓您使用歷史&事件 模組。

- 立即更新

  開始更新安裝在此電腦上的BitDefender 產品。

- 設定此電腦為此網路的更新伺服器

  讓您能夠設置這台電腦為整個網路中的BitDefender更新伺服器。 使用這個選項將會減少網路傳輸，因為只有一台電腦會連上網路下載更新。

在執行特定電腦的任務以前，將提示您輸入本地家庭管理密碼。



輸入密碼

輸入家庭管理密碼，並點擊確定。



註

若您要執行多個任務，您可以選擇這段期間不要再顯示這個訊息。 這樣，這段期間將不會再提示您輸入密碼。

24. 更新

每一天都有新的惡意程式被發現及識別。這就是為什麼 BitDefender 需要保持最新的病毒特徵碼是非常重要的。預設上，BitDefender 是每個小時自動檢查更新。

如果您是透過寬頻或 ADSL 連線到網際網路，BitDefender 會特別注意更新。當您啟動您的電腦後，它將每 小時 確認更新。

自動更新設定。

更新程序正在進行中，代表原有的檔案正在被更新的檔案取代。在更新的同時，產品也不會有弱點。

更新會利用以下幾種方式：

- 病毒引擎更新 — 更新最新的病毒碼。這個更新的型態是我們熟知的 病毒定義更新。
- 反間諜程式引擎更新 — 新的間諜程式特徵碼將會被加入到資料庫。這個更新的型態是我們熟知的 反間諜程式更新。
- 軟體更新 — 當一個新的軟體版本被發行時，新的功能的掃描技術都用以提升軟體的效能，這個更新的型態是我們熟知的 軟體更新。

24.1. 自動更新

要檢視更新的相關資訊並執行自動更新，請在進階檢視選擇更新>更新。



自動更新

您可以在此檢視最近一次的更新是何時進行的、更新時是否成功。防毒引擎的版本資訊以及所有的特徵碼數量也會在此顯示。

如果您在更新的過程開啟此頁面，您將能夠檢視狀況。



重要

為了防護您的系統以抵抗最新的病毒威脅，請保持 自動更新 啟動。

24.1.1. 正在要求更新

點擊Update Now以隨時在您想要的時候進行自動更新。這個更新的型態是我們熟知的使用者要求的更新。

這個 更新 模組將連線到 BitDefender 更新伺服器並且確認是否有更新可用。如果偵測到一個更新，將依據 手動更新設定 頁面的設定，您將被詢問是否要執行更新或者自動地安裝更新。



重要

當您完成更新時，可能需要將電腦重新啟動。我們建議盡可能重新開機。



註

如果您是利用撥接方式連線到網際網路，建議您定期地更新 BitDefender 以獲得最好的防護效果。

24.1.2. 停用自動更新

如果您關閉自動更新，您將會收到一個警告視窗。 您可以從視窗選擇您要停用自動更新的時間長度。您可以選擇：5分鐘、15分鐘、30分鐘、一個小時、永久停用、或是直到下次系統重新開機。



警告

這將會是個重大安全事件，我們建議您盡可能減少停用自動防護的時間。如果BitDefender無法正常地執行更新，它將無法防護您的電腦抵抗最新的威脅。

24.2. 更新設定

可以從本地網路、或直接連線到網際網路或透過 Proxy 伺服器進行更新。 預設上，BitDefender能夠每小時檢查是否有新的可用更新並且能夠自動下載安裝到您的電腦。

要設置更新設定與管理proxy，請在進階檢視選擇更新>設定。

更新設定

在更新設定的視窗包含四個類型的選項 (更新位置設定、自動更新設定、手動更新設定 及 進階設定) 以可展開的選單方式呈現。

24.2.1. 更新位置設定

設定更新位置。這個設定透過更新位置設定目錄來進行。



註

設置這些設定，只有當如果您連接到地方性地儲存 BitDefender 惡意軟體驗證的一個本地區域網路，或者如果您經過一個proxy伺服器(Proxy)對網際網路連接。

為了更穩定及更快速地更新，您可以設定二個更新位置：一個是 主要的更新位置，另一個是 次要的更新位置。這兩個預設都是 http://upgrade.bitdefender.com。

要修改更新位置，在對應的URL欄位提供鏡像位置的URL。



註

我們推薦您設置主要更新位置為您身處的地區的鏡像，讓其他更新位置保持不變，以防萬一連不到本地的鏡像。

通常，公司會使用proxy伺服器連接網際網路，把使用proxy 打勾，並點擊管理proxy 設置proxy設定。 更多資訊，請參閱 "管理Proxy" (p. 168)

24.2.2. 調整自動更新

要設置BitDefender的自動更新程序，使用自動更新設定裡的選項。

您可以在時間間隔的欄位設定一段時間。預設上，更新時間間隔為一小時。

要指定自動更新如何執行，請選擇下列項目：

- 靜態更新 — BitDefender 自動地下載及執行更新。
- 在下載更新前提示 — 每次當有更新可用時，在下載前先詢問您。
- 在安裝更新前提示 — 每一次有下載更新時，在安裝前先詢問您。

24.2.3. 設置手動更新

要調整BitDefender的手動更新程序，選取手動更新設定裡的選項：

- 隱匿更新 — 手動更新將自動地執行不會顯示使用介面。
- 在下載更新前提示 — 每次當有更新可用時，在下載前先詢問您。

24.2.4. 設置進階設定

要避免BitDefender更新程序影響您的作業，請設置在進階設定目錄裡的選項：

- 等待重新開機以取代提示 — 如果一個更新要求重新開機時，軟體將仍以舊的檔案繼續運作，直到系統被重新開機。使用者將不會被提示重新開機，因此 BitDefender 更新程序將不會妨礙使用者的工作。

- 掃描中不要執行更新 — 如果正在執行掃描程序，BitDefender 將不會進行更新。這樣 BitDefender 更新程序將不會影響掃描工作。



註
當掃描正在進行時，如果 BitDefender 執行更新，則掃描程序將會被終止。

- 如果開啟遊戲模式，請勿更新 — 如果BitDefender遊戲模式設為開啟，則不會執行更新。 如此，您變能夠將遊戲影響最小化。

24.2.5. 管理Proxy

若您的公司使用proxy伺服器上網，您一定要設置proxy設定使BitDefender可以自己更新。否則，它會使用裝了產品的管理者proxy設定



註
Proxy設定只能被有管理權限的使用者調整(完整控制模式)。

要管理proxy設定，點擊Proxy設定。將會出現一個新視窗。

BitDefender Proxy 設定
安裝時偵測到的Proxy
位址： 接埠： 使用者名稱：
密碼：
預設的瀏覽器Proxy
位址： 接埠： 使用者名稱：
密碼：
自訂的Proxy
位址： 接埠： 使用者名稱：
密碼：
您可以在這裡設定在安裝時偵測到的Proxy設定。
確定 取消

Proxy 管理員

Proxy設定有三組類別：

- 管理者proxy設定(偵測於安裝時間) – 在安裝時偵測管理者帳號內的proxy設定，只有當您登入到該帳號時才能設置proxy。如果proxy伺服器需要一個使用者名稱和一個密碼，您一定要在對應的欄位中填上。
- 預設瀏覽器Proxy - 目前使用者的proxy設定，由預設瀏覽器中取得。如果proxy伺服器需要使用者名稱和密碼，您必須在對應的欄位輸入。



註
支援的瀏覽器有Internet Explorer, Mozilla Firefox 和 Opera。若您預設使用其他的瀏覽器，BitDefender就不能夠讀取目前使用者設定。

- 自訂的proxy設定 — 當您以系統管理者登入時，您可以調整的proxy設定。

  以下的選項是必須被指定的：
  - 位址 — 輸入proxy伺服器的IP。
  - 連接埠 — 輸入BitDefender 要使用連接到 Proxy 伺服器的連接埠。
  - 使用者名稱 — 輸入 Proxy伺服器可識別的使用者名稱。
  - 密碼 — 輸入先前指定使用者的有效密碼。

當嘗試連接到網路，每一組的proxy伺器設定都會去試，直至BitDefender連上。

首先，您自行設置的proxy設定會先連上網。若連不到，就會嘗試用在安裝時所讀取到的proxy設定來試。最後，如果都不行，就會用目前使用者預設瀏覽器的proxy來上網。

按 確定 儲存這個設定並關閉視窗。

點擊 套用－儲存變更或點擊 預設 載入預設值。

25. 註冊

要取得您的BitDefender完整資訊及註冊狀態，請在進階檢視選擇註冊。



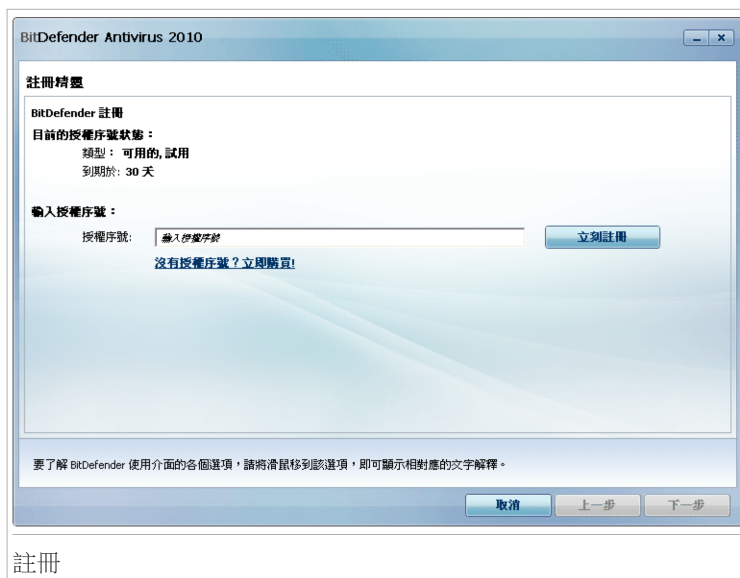
註冊

這個頁面顯示：

- 產品資訊：BitDefender的產品版本。
- 註冊資訊：用來登入您的BitDefender帳號的電子郵件位址，目前的授權序號，以及還有幾天序號將會到期。

25.1. 註冊BitDefender 病毒防護 2010

點擊立刻註冊以開啟產品註冊視窗。



註冊

您可以檢視BitDefender 註冊狀態，現在使用的授權序號，以及授權序號將在幾天內到期。

註冊BitDefender 病毒防護 2010：

1. 在編輯欄位中輸入授權序號。



註

您可以在這些地方找到授權序號：

- 光碟標籤。
- 產品註冊卡。
- 線上購買的電子郵件。

如果您沒有BitDefender的授權序號，您可以連線至BitDefender 線上商店購買授權序號。

2. 點擊立即註冊。
3. 點擊 完成。

25.2. 建立一個 BitDefender 帳號

建立一個 BitDefender 帳號是註冊程序的重要步驟。 透過BitDefender帳號，您可以享有免費的更新服務、專業技術支援及特別的續購優惠。 如果您遺失了BitDefender授權序號，您可以透過http://myaccount.bitdefender.com並登入您的帳號以重新取得您的授權序號。



重要

您必須在安裝BitDefender15天內建立一個帳號(試用期將會被延長至30天)。 否則，BitDefender將不再繼續更新。

如果您還沒有建立BitDefender帳號，點擊啟動產品以開啟帳號註冊視窗。

建立帳號

如果您不想建立 BitDefender 帳號，選取 稍候註冊並點擊完成。 否則，根據您目前的狀況選擇：

- “我沒有BitDefender 帳號” (p. 172)
- “我已經擁有BitDefender 帳號。” (p. 173)

我沒有BitDefender 帳號

要順利建立BitDefender帳號，請依循下列步驟：

1. 選取建立一個新帳號。
2. 在對應的欄位輸入必要的資訊。 您在這裡所提供的資料將會被保密。
   - E-mail address — 輸入您的電子郵件信箱。
   - 密碼 — 為您的BitDefender帳號輸入一組密碼。 密碼長度必須要有6-16個字元。
   - 重複鍵入密碼 — 重新輸入先前的密碼。



註

一旦帳號被啟用，您可以http://myaccount.bitdefender.com輸入您的電子郵件位址與密碼登入帳號。

3. 您可以在BitDefender帳號所登記的電子郵件信箱，收到特別的續購優惠的相關訊息。 從選單選取一個選項：
   - 傳送所有訊息
   - 只傳送給我產品相關的訊息
   - 不要傳送任何訊息
4. 點擊建立。
5. 點擊完成 以關閉精靈。
6. 啟用您的帳號。. 在能夠您的帳號前，您必須先啟動。 檢查您的EMAIL並且依循信中的BitDefender registration service指示完成程序。

我已經擁有BitDefender 帳號。

BitDefender 將會自動發現您先前電腦上登記的 BitDefender 帳號。 在這個狀況，請提供您的帳號密碼並點擊登入。 點擊完成 以關閉精靈。

若您已經擁有一個啟動的帳號，但BitDefender沒有偵測到，請依循這些步驟註冊：

1. 點選登入(先前註冊的帳號)。
2. 在對應的欄位輸入電子郵件位址與密碼。



註

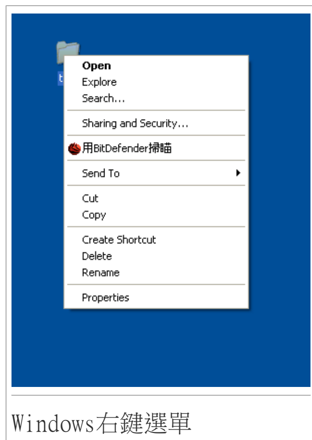
如果您忘記您的密碼，點擊 忘記您的密碼？ 並依循指示操作。

3. 您可以在BitDefender帳號所登記的電子郵件信箱，收到特別的續購優惠的相關訊息。 從選單選取一個選項：
   - 傳送所有訊息
   - 只傳送給我產品相關的訊息
   - 不要傳送任何訊息
4. 點擊登入。
5. 點擊完成 以關閉精靈。

整合Windows 和第三方軟體

26. 整合Windows右鍵選單

在當您在Windows按下滑鼠右鍵時，會出現右鍵選單。



Windows右鍵選單

BitDefender與右鍵選單整合，如此您可以更方便掃描可疑檔案。 在右鍵選單的BitDefender 圖示，您可迅速找到掃描選項。

26.1. 用 BitDefender 掃瞄

使用右鍵選單功能，您可以輕易地掃描檔案、資料夾，或是整個硬碟。 在您想要掃描的檔案或目錄按下滑鼠右鍵，並選擇 用 BitDefender 掃描。 病毒掃描精靈會出現並引導您完成整個掃瞄過程。

掃描選項. 掃描選項是為了最佳的掃描效果而設置。 若偵測到受感染的檔案，BitDefender 將會嘗試解毒。 若消毒失敗，病毒掃描精靈將會允許您採取其他動作。

如您想更改掃描選項，請按照以下步驟：

1. 開啟BitDefender 並將使用者介面切換至進階模式。
2. 從左側選單點擊 病毒防護。
3. 點擊 病毒掃描標籤。
4. 滑鼠右鍵點選右鍵選單掃描任務並點選開啟。 一個新的視窗將會出現。
5. 點擊自定並設置需要的掃描選項。 將滑鼠移到要了解的選項，畫面下方即會出現相關的描述。
6. 點擊確定 去儲存變更。
7. 點擊確定確認並套用新的設定。



重要
您不應該變更這個掃描任務的設定。

27. 整合入網頁瀏覽器

BitDefender能夠防護您的電腦免於網路釣魚的威脅。 它能夠掃描您正在瀏覽的網站，並警告您有網路釣魚的威脅。 您可以設定網站白名單，如此BitDefender將不會掃描這些網站。

BitDefender 將功能整合，透過一個直覺且易於使用的工具列進入下列瀏覽器：

- Internet Explorer
- Mozilla Firefox

您可以輕易的使用整合入上列瀏覽器的BitDefender反網路釣魚工具列，管理反網路釣魚防護功能及白名單。

反網路釣魚工具列位於瀏覽器的上方，以BitDefender 圖示表示。 要開啟工具列選單，請點擊這裡。



註
如果您無法看見工具列，開啟 檢視 選單，選擇工具列並選取BitDefender 工具列。



反網路釣魚工具列

在工具列選單會有以下可用的命令：

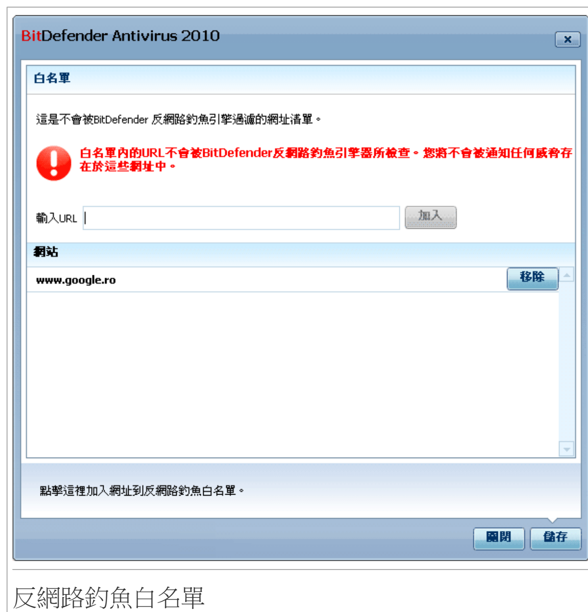
- 啟動 / 停用 - 啟動 / 停用 BitDefender反網路釣魚工作列。
- 設定 - 開啟一個視窗，您可以調整反網路釣魚工作列的設定。 有以下選項可選：
  - □即時反網路釣魚防護 - 即時提醒您網頁中可能的釣魚危險。 此選項只控制瀏覽器的BitDefender反網路釣魚防護。
  - □加入白名單前先詢問 - 在您將網站加入白名單前，先詢問您。

- 加入白名單 - 將目前的網站加入白名單。



註
將網站加入白名單意謂著BitDefender將不會再針對該網站使用反網路釣魚功能。建議您只將您絕對信任的網站加入。

- 白名單 — 開啟白名單。



反網路釣魚白名單

您可以查看所有不會被BitDefender反網路釣魚引擎掃描的網站。 假如您要從白名單中移除任何網站使您可以得知此網站是否有網路釣魚威脅，點擊他旁邊的移除按鈕。

您可以將您絕對信任的網站加入白名單，如此這些網站將不會在被反網路釣魚引擎掃描。 要將網站加入白名單，在所對應的欄位輸入網站的網址並點擊加入。

- 報告網路釣魚 - 告知BitDefender Lab您認為此網站被用作網路釣魚用途。 藉由回報釣魚網站，您可以幫助其他人不受到身分遭竊的威脅。
- 說明 - 開啟一個說明檔。
- 關於 - 開啟一個視窗，在此您可以得到更多關於BitDefender的資訊，並尋求相關協助。

28. 整合即時通訊程式

BitDefender提供加密功能，防護您的機密文件和您透過Yahoo即時通與MSN Messenger的即時交談對話。

BitDefender加密所有您的即時交談訊息，預設規定：

- 您的交談對象已安裝了支援即時通訊加密的BitDefender版本，並且即時通訊加密在您的即時通訊程式上已經啟動。
- 您和您的交談對象使用Yahoo即時通或是Windows Live (MSN) Messenger交談。

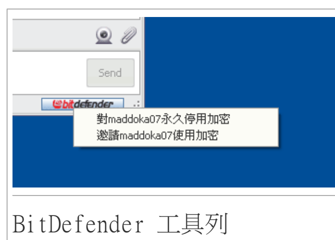


重要
若您的交談對象使用，如Meebo、或其他支援Yahoo即時通與Windows Live (MSN) Messenger的網頁型的交談程式，BitDefender將無法加密對話。

您可以從交談視窗中使用BitDefender工具列，輕易的設置即時通訊加密。 工具列會位於交談視窗的右下方。



註
若交談已加密，您會看到工具列旁有一個鑰匙圖示。



BitDefender 工具列

點擊BitDefender工具列，將提供您下列的選項：

- 對 聯絡人永久停用加密。.
- 邀請 聯絡人使用加密。. 要加密您的對話，您的聯絡人必須也安裝BitDefender並使用相容的即時通訊程式。

如何

29. 如何掃描檔案與資料夾

您可以輕易地使用BitDefender 掃描您的系統 有四種方式可以設定使用BitDefender 掃描您的檔案與資料夾:

- 使用 Windows 右鍵選單
- 使用掃描任務
- 使用 BitDefender 手動選擇掃描
- 使用掃描活動列

當您開始啟動掃描，掃描精靈將會出現並指引您完成所有流程。 要了解更多資訊，請參考 “病毒掃描精靈” (p. 46)。

29.1. 使用Windows右鍵選單

這是最簡單的掃描方式。 在您想要掃描的檔案或目錄按下滑鼠右鍵，並選擇 用 BitDefender 掃描。 依循病毒掃描精靈的只是完成掃描。

您會需要使用此掃描方式的情況為:

- 您懷疑一個檔案或資料夾遭受感染。
- 當您懷疑從網站上下載的檔案可能受到感染時，
- 在複製到您的電腦前掃描網路共享的檔案。

29.2. 使用掃描任務

若您需要時常掃描您的電腦或是特定的資料夾，您應該考慮使用掃描任務。 掃描任務可以設定要掃描的時間以及要被掃描的位置。 您可以使用排程 功能設定執行掃描的時間。

要使用掃描任務掃描您的電腦，您必須開啟產品主畫面並選擇要執行的任務。 根據使用的不同使用者介面檢視模式，在執行掃描任務時也有不同的步驟。

在一般模式執行掃描任務

在新手模式中，你只能夠透過點擊 立刻掃描以執行一個標準的掃描。 依循病毒掃描精靈的只是完成掃描。

在一般模式執行掃描任務

在一般模式中，您可以進行幾個事先設置過的掃描任務。您也可以設置並執行一個自訂的掃描任務，以指定的選項掃描特定的電腦位置。 依循這些步驟在一般模式執行掃描任務：

1. 點擊 病毒防護標籤

2. 在左邊的快速任務區域，點擊系統掃描已開始一個標準的全電腦掃描。要執行不同的掃描任務，點擊按鈕上的箭頭並選取想要的掃描任務。 要設置與執行自定掃描，點擊自定掃描。 下列是可用的掃描任務:

掃描任務	描述
系統掃描	掃描整個系統，資料封存除外。 在預設的設定中，它將掃描除了後門程式之外的所有惡意程式類型。
深度系統掃描	掃描整個系統。 在預設的設置中，它能夠掃描您電腦中所有種類的惡意威脅。
我的文件掃描	使用這個掃描任務執行掃描重要的使用者資料夾，如：我的文件 、桌面 以及 開始功能表。
自訂掃瞄	此選項協助您設置並執行系統掃描，您可以選擇要掃描的項目與設定掃描的選項。 您可以儲存掃描任務以便稍後可在一般模式與進階檢視模式進行存取。

3. 依循病毒掃描精靈的只是完成掃描。 若您選了一個自定任務，您必須完成自定掃描精靈。

在進階模式執行掃描任務

在進階檢視，您可以執行所有預設好的任務，並可以變更設定。 此外，您也可以建立符合您需求的任務。 依循這些步驟在進階檢視執行掃描任務：

1. 從左側選單點擊 病毒防護。
2. 點擊 病毒掃描標籤。 您可在此找到預設任務並建立自定的掃描任務。 這些是您可以使用的預設任務：

預設的任務	描述
深度系統掃描	掃描整個系統。 在預設的設置中，它能夠掃描您電腦中所有種類的惡意威脅。
系統掃描	掃描整個系統，資料封存除外。 在預設的設定中，它將掃描除了後門程式之外的所有惡意程式類型。
快速的系統掃描	掃描Windows與Program Files資料夾。 在預設的設定中，可以掃描除後門程式外所有的惡意程式，但是不會掃描記憶體、登錄碼、cookies.
我的文件	使用這個掃描任務執行掃描重要的使用者資料夾，如：我的文件 、桌面 以及 開始功能表。

3. 在您要執行的任務點擊兩下滑鼠。

4. 依循病毒掃描精靈的只是完成掃描。

29.3. 使用 BitDefender 手動選擇掃瞄

BitDefender手動掃描任務讓您可以指定要掃描的資料夾或是硬碟。 這個功能是設計用來在Windows的安全模式執行。 若系統被感染病毒，您可以嘗試在Windows安全模式之下使用手動掃描功能，偵測病毒並嘗試解毒。

要用手動選擇掃描任務掃描您的電腦，依循這些步驟:

1. 到 start Windows 開始功能表，路徑:開始 → 程式集 → BitDefender 2010 → BitDefender 手動選擇掃描。 將會開啟一個新的視窗。
2. 點擊加到資料夾選取掃描目標。 將會開啟一個新的視窗。
3. 選擇掃描目標：
   - 要掃描您的桌面，請選擇桌面。
   - 要掃描整個磁碟分割，請從我的電腦磁碟清單選擇。
   - 要掃描一個資料夾，點選瀏覽。
4. 按下確定。
5. 點擊繼續 以開始掃描。
6. 依循病毒掃描精靈的只是完成掃描。

什麼是安全模式?
安全模式是專為Windows發生問題時所使用的開機模式， 在安全模式下，Windows只會啟動最基本的元件與驅動程式。大部分的程式都無法在安全模式啟動，所以可以在安全模式下將病毒順利刪除。
在電腦開機時，按下F8鍵，即可進入安全模式選單。若您要在安全模式下能夠存取網路，請選擇安全模式 含網路功能選項。



註

要了解更多資訊，請到開始功能表，點選說明與支援。 您也能在網路上找到有用的資訊。

29.4. 使用掃描活動列

這個 掃描活動列 是您的系統上掃描活動的圖形。 這個小視窗只預設會出現於進階模式。

您可以使用掃描活動列掃描檔案與資料夾。 將要掃描的檔案或資料托放到掃描活動列。 依循病毒掃描精靈的只是完成掃描。



掃瞄活動列



註

要了解更多資訊，請參考"掃瞄活動列" (p. 26)。

30. 如何排程電腦掃描

定期地掃描您的電腦以免除惡意程式威脅。 BitDefender讓您可以排程掃描任務於您的電腦自動執行掃描任務。

要排程掃描任務，請依循下列步驟：

1. 開啟BitDefender 並將使用者介面切換至進階模式。
2. 從左側選單點擊 病毒防護。
3. 點擊 病毒掃描標籤。 您可在此找到預設任務並建立自定的掃描任務。
   - 系統任務可於不同的Windows帳號執行。
   - 使用者任務只能於建立該任務的使用者帳號才能使用。

   這些是您可以排程的預設任務：

預設的任務	描述
深度系統掃描	掃描整個系統。 在預設的設置中，它能夠掃描您電腦中所有種類的惡意威脅。
系統掃描	掃描整個系統，資料封存除外。 在預設的設定中，它將掃描除了後門程式之外的所有惡意程式類型。
快速的系統掃描	掃描Windows與Program Files資料夾。 在預設的設定中，可以掃描除後門程式外所有的惡意程式，但是不會掃描記憶體、登錄碼、cookies.
自動登入掃描	掃描使用者登入Windows就執行的項目。 要使用此任務，您必須排程它於系統啟度時執行。 自動登入掃描預設為停用的。
我的文件	使用這個掃描任務執行掃描重要的使用者資料夾，如：我的文件 、桌面 以及 開始功能表。

   若這些任務不符合您的需求，您可以建立一個自定的掃描任務。

4. 右鍵點擊掃描任務並選取排程。 將會開啟一個新的視窗。
5. 排程任務在需要時執行：
   - 若您要一天執行一次，選擇一次並指定開始的日期與時間。
   - 要在系統啟動後執行掃描任務，請選取在系統啟動時。 您可指定在系統啟動多久(分鐘)之後開始執行。
   - 若您要規則的執行任務，選擇週期地並指定頻率與開始的日期時間。



註
例如：要於每星期六早上兩點執行掃描，您必須依照下列說明：

a. 點擊週期的。

b. 在每逢欄位，輸入1並選擇星期。 如此，這個任務便會每星期運行一次。

c. 將開始日期設在即將來臨的星期六。

d. 開始時間設為2:00:00 AM。

6. 點擊確定 儲存排程。 掃描任務會自動在您排程的時間執行。 若到了排程的時間但是電腦沒有啟動，任務會在您下次開機時執行。

問題排除並取得協助

31. 排除問題

這個章節告訴您在使用BitDefender 過程中可能出現的問題，以及可能的解決方案。大部份的問題都可以透過正確的產品設置解決。

如果您無法找到您的問題，或是提供的解決方法無法解決問題，您可以聯絡BitDefender技術支援"支援" (p. 191)。

31.1. 安裝問題

此文章協助您排除常見的安裝問題。 這些問題會被分類成以下類別：

- 安裝驗證錯誤：設定精靈因為電腦的狀況無法正常執行。
- 安裝失敗：您開始安裝精靈後，作業沒有成功完成。

31.1.1. 安裝驗證錯誤

當您開始設定精靈，將會有一連串的驗證作業來判定安裝是否能開始執行。 下列表格顯示最常見的安裝驗證錯誤與排除的方法。

錯誤	描述&解決方案
您沒有足夠的權限安裝程式。	要執行設定精靈並安裝BitDefender您需要管理者權限。您可以選擇以下動作： ● 登入Windows管理帳號並再執行一次安裝程序。 ● 在安裝檔點擊右鍵並選擇以...執行。 輸入必要的帳號密碼資訊。
安裝程式偵測到先前的BitDefender產品沒有移除乾淨。	先前安裝在您電腦的BitDefender產品沒有適當地移除，這樣影響新的安裝， 要排除錯誤並安裝BitDefender，請依循下列步驟： 1. 到www.bitdefender.com/uninstall下載並儲存移除工具。 2. 使用管理者權限執行移除工具。 3. 重新啟動電腦。 4. 再次開啟設定精靈並安裝BitDefender。
BitDefender產品與您的作業系統不相容。	您可以嘗試安裝BitDefender在沒有支援的作業系統。請檢查"系統需求" (p. 2)找到可以安裝BitDefender的作業系統。

錯誤	描述&解決方案
	若您的Windows XP只有SP1，您必須安裝SP2或以上的版本並再執行設定精靈。
安裝檔案可於不同的處理器使用。	若您得到這樣的錯誤，您可能是執行不正確的安裝檔。BitDefender安裝檔有兩個版本：32位元/64位元。 您要確認正確的版本，請直接到http://www.bitdefender.com/links/sg/homepage.html下載安裝檔。

31.1.2. 安裝失敗

安裝失敗有幾可能性：

- 安裝期間出現錯誤畫面。 您會看見一個視窗，在此您可以選擇取消或執行移除工具清除系統。



註
當您開始安裝作業，您會被告知沒有足夠的磁碟空間可安裝BitDefender。您必須先釋放出必要的磁碟空間，並再繼續或重新開始安裝作業。

- 安裝停滯或是您的系統當機。 請重新啟動電腦。
- 安裝已完成，但你無法使用BitDefender的功能。

要排除安裝是拜的問題並安裝BItDefender，請依循下列步驟：

1. 安裝失敗時清理電腦系統。. 若安裝失敗，BitDefender登錄檔可能會留在您的系統中，這些殘留的項目會影響新的安裝也可能影響系統運行。您必須先將這些項目移除才能再重新安裝。

   若錯誤畫面提供一個移除工具，請執行移除工具清理您的系統。 否則，請執行下列步驟：

   a. 到www.bitdefender.com/uninstall下載並儲存移除工具。

   b. 使用管理者權限執行移除工具。

   c. 重新啟動電腦。

2. 確認可能的失敗原因。. 在繼續安裝前，請確認可能會導致安裝錯誤的肇因：

   a. 檢查若您在電腦上有安裝其他防毒產品，他們會導致BitDefender作業不正常。進議您移除其他防毒產品再安裝BitDefender。

   b. 您也應該檢察系統是否受到感染。 您可以選擇以下動作：

      - Use the BitDefender Rescue CD to scan your computer and remove any existing threats. 要了解更多資訊，請參閱“BitDefender 救援光碟” (p. 194)。

- 開啟IE瀏覽器，到www.bitdefender.com並執行線上掃描(點擊scan online 按鈕)。

3. 嘗試重新安裝BitDefender。 建議您下載並執行最新版本的安裝檔 http://www.bitdefender.com/links/sg/homepage.html。
4. 若安裝再次失敗，請聯絡 BitDefender以取得協助“支援” (p. 191)。

31.2. BitDefender 服務沒有回應

這裡幫助您排除BitDefender服務沒有回應的錯誤。 您可能如以下發生這些錯誤：

- 系統工具列的BitDefender圖示已變成灰色，並顯示BitDefender服務已沒有回應。
- BitDefender 主畫面會顯示BitDefender服務已沒有回應。

這個錯誤可能由下列其中一個情況造成：

- 已安裝重要的更新。
- 暫時與BitDefender 服務的傳輸錯誤。
- 部份BitDefender 服務已停止。
- 同時間有其他防毒產品在系統上執行。
- 電腦上的病毒影響BitDefender正常運作。

要排除這個錯誤，嘗試這些解決方法：

1. 稍待一會再看看有沒有任何改變。 錯誤可能是暫時的。
2. 重新啟動電腦並等待BitDefender 載入。如果問題持續存在請開啟BitDefender 。重新啟動電腦通常能夠解決這個問題。
3. 檢查若您在電腦上有安裝其他防毒產品，他們會導致BitDefender作業不正常。進議您移除其他防毒產品再安裝BitDefender。
4. 若錯誤依舊持續，可能會示更嚴重的問題，例如：感染的病毒會干預BitDefender運作。 請聯絡 BitDefender以取得協助“支援” (p. 191)。

31.3. BitDefender 移除失敗

本文協助您解決移除BitDefender時所發生的問題。 有兩種可能的狀況：

- 移除期間出現錯誤畫面。 在視窗出現一個按鈕可以執行移除工具。
- 移除作業停滯或是您的系統當機。 點擊取消中止移除作業。若沒有作用，請重新啟動電腦。

若移除失敗，BitDefender登錄檔可能會留在您的系統中，這些殘留的項目會影響新的安裝也可能影響系統運行。您必須先將這些項目移除才能再重新安裝。 要從系統完整地移除BitDefender，您必須執行移除工具。

若移除失敗且出現錯誤畫面，點擊移除工具按鈕並清理您的系統。 否則，請執行下列步驟：

1. 到www.bitdefender.com/uninstall下載並儲存移除工具。
2. 使用管理者權限執行移除工具。 移除工具會把所有在自動移除程序中不能移除的檔案及登錄鍵移除。
3. 重新啟動電腦。

若此資訊無法協助您，請聯絡BitDefender以取得協助“支援” (p. 191)。

32. 支援

BitDefender積極地提供客戶最迅速且有效率的支援服務。 BitDefender線上支援資料庫提供客戶詳細的說明解決大部分的常見問題。 若資料庫找不到解決方案，客戶可以用線上顧客服務，我們的專業人員將會協助您解決此問題。

32.1. BitDefender 知識庫

BitDefender 知識庫是一個關於 BitDefender 產品的線上資訊庫。它利用很簡單易於存取的格式、由 BitDefender 支援及研發團隊提供不間斷的技術支援及錯誤修正、關於病毒預防的一般主題、詳細解釋 BitDefender 解決方案及其他更多的主題。

BitDefender 知識庫是公開並可自由地搜尋。它廣泛的資料包含提供買了BitDefender的消費者所需技術上的知識。所有有效的資料請求或臭蟲報告都是來自BitDefender的客戶。通常他們都能從BitDefender 知識庫，如 bugfix 報告、工作區、圖表 或者資訊的文章提供額外的支援。

BitDefender 知識庫可以在任何時間進行存取 http://kb.bitdefender.com。

32.2. 要求幫助

要尋求協助，您必須使用BitDefender網路自助服務。只要依循下列步驟：

1. 請到http://www.bitdefender.com/help。 您可在此找到BitDefender線上資料庫。BitDefender線上資料庫包含了許多與產品相關問題的解決方案。
2. 搜尋資料庫的說明文章可以提供您解決方案。
3. 請閱讀相關文章並嘗試找到解決方案。
4. 若您無法找到解決方案，請用文章裡的連結聯繫BitDefender顧客服務。
5. 登入您的BitDefender 帳號。
6. 使用EMAIL、電話、即時通訊，聯絡BitDefender技術人員。

32.3. 聯絡資訊

有效率的溝通是成功事業的關鍵。在過去十年中，BITDEFENDER已經建立一個無懈可擊的信譽，歷經不斷地努力溝通，超越客戶及夥伴的期望。如果您有任何問題，都希望不吝與我們聯絡。

32.3.1. 網站位址

業務部門：sales@bitdefender.com
技術支援：www.bitdefender.com/help
檔案相關問題：documentation@bitdefender.com
夥伴計劃：partners@bitdefender.com

市場行銷 marketing@bitdefender.com
媒體相關：pr@bitdefender.com
工作機會：jobs@bitdefender.com
病毒遞交：virus_submission@bitdefender.com
垃圾郵件遞交：spam_submission@bitdefender.com
報告濫用：abuse@bitdefender.com
產品網站：http://www.bitdefender.com
產品檔案FTP位址：ftp://ftp.bitdefender.com/pub
當地代理商：http://www.bitdefender.com/partner_list
BitDefender 知識庫：http://kb.bitdefender.com

32.3.2. 當地代理商

BitDefender 的代理商已經準備好回應任何產品相關的諮詢，無論在商務或其它事件。

電話: +886 (02) 2365 0238
傳真: +886 (02) 2365 0196
電子郵件: service@qcomgroup.com.tw
購買: http://www.bitdefender.com/links/sg/buy/antivirus.html
技術支援: http://bitdefender.qcomgroup.com/cnt2010/support/
網站:http://www.bitdefender.com/links/sg/homepage.html

32.3.3. BitDefender 聯絡窗口

BitDefender辦公室已經準備好回應關於他們的任何諮詢，無論在商業或更大的事件。他們的地址和連絡方式在下面被列出。

美國

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
電話(office&sales)： 1-954-776-6262
銷售： sales@bitdefender.com
技術支援： http://www.bitdefender.com/help
網站: http://www.bitdefender.com

Germany

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
聯絡窗口: +49 2301 91 84 222

銷售： vertrieb@bitdefender.de
技術支援： http://kb.bitdefender.de
網站: http://www.bitdefender.de

英國及愛爾蘭

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
電子郵件： info@bitdefender.co.uk
電話: +44 (0) 8451-305096
銷售： sales@bitdefender.co.uk
技術支援： http://www.bitdefender.com/help
網站: http://www.bitdefender.co.uk

Spain

BitDefender España SLU
C/ Balmes, 191, 2º, 1ª, 08006
Barcelona
傳真: +34 932179128
電話: +34 902190765
銷售： comercial@bitdefender.es
技術支援： www.bitdefender.es/ayuda
網站： http://www.bitdefender.es

羅馬尼亞

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
傳真: +40 21 2641799
業務專線： +40 21 2063470
E-mail: sales@bitdefender.ro
技術支援： http://www.bitdefender.ro/suport
網站： http://www.bitdefender.ro

BitDefender 救援光碟

33. 總覽

BitDefender 病毒防護 2010 含有可開機光碟，在您的作業系統啟動前，可進行掃描及清除所有存在的磁碟機。

您可以在您的作業系統因為病毒而無法運作時，使用 BitDefender 救援光碟。當您未使用任何病毒防護產品時，這種情形會常常發生。

病毒特徵碼的更新會自動進行，不需要在您每次啟動 BitDefender 救援光碟時再進行更新。

BitDefender 救援 CD提供一個桌面以供掃描及清除NTFS硬碟上的病毒之用。同時BitDefender在您不用進入可以Windows時，還原您的資料。



註
BitDefender救援光碟可於下列位置下載：http://download.bitdefender.com/rescue_cd/

33.1. 系統需求

在使用 BitDefender 救援 CD 開啟電腦前，您必須先確認您的系統符合以下的需求。

CPU 種類
: x86 相容機種、最少需要 166 MHz，但不能期望有很好的效能。i686 系列的處理器、800 MHz，可能運作的更有效率。

記憶體
: 最少 512MB 記憶體或以上 (建議使用1GB)

光碟機
: BitDefender救援光碟是由光碟機執行，因此，光碟機及可以從 BIOS 啟動開機為其要求項目。

網際網路連線
: 雖然BitDefender救援光碟是不需要在網際網路連線下執行，但更新的程序會要求啟動 HTTP 連線，甚至可以透過 Proxy 伺服器。因此，為了提供完整的防護，網際網路的連線是必需的。

圖形介面的解析度
: 標準 SVGA-相容圖像顯示卡

33.2. 包含的軟體

BitDefender 救援光碟包含以下的軟體程式。

Xedit
: 這是文字檔案編輯器。

Vim
這是更強的文字檔案編輯器，包含強調的語法格式，圖形用戶界面。要更多資訊，請參閱Vim網站。

Xcalc
這是計算機。

RoxFiler
RoxFiler是一個快速而強大的圖形檔案管理員

想要更多資料，請瀏覽 RoxFiler網站。

MidnightCommander
GNU Midnight Commander (mc)是一個文字介面檔案管理員。

想要更多資料，請瀏覽 MC網頁。

Pstree
Pstree顯示正在執行的程序。

Top
上方顯示Linux工作區。

Xkill
Xkill用來強制關閉系統中的任何一個應用程式。

Partition Image
Partition Image幫您儲存整個分割區(EXT2, Reiserfs, NTFS, HPFS, FAT16, and FAT32)至一個映像檔。此軟體能協助您備份。

要更多資料，請瀏覽Partimage網頁.

GtkRecover
GtkRecover是個GTK版本的檔案復原工具。它能助您挽回檔案。

要更多資料，請參閱GtkRecover網頁。

ChkRootKit
ChkRootKit能助您掃描電腦內的rootkit。

要更多資料，請參閱ChkRootKit 網頁.

Nessus Network Scanner
Nessus是一個Linux, Solaris, FreeBSD, and Mac OS X遠端安全掃描器。

要更多資料，請參閱Nessus網頁。

Iptraf
Iptraf是個IP網路監控軟體。

要更多資料，請參閱Iptraf網頁。

Iftop
Iftop顯示每個介面的頻寬用量。

要更多資料，請參閱Iftop 網頁。

MTR
MTR是一個網路診斷工具。

要更多資料，請參閱MTR網頁

PPPStatus
PPPStatus顯示TCP/IP流出流入的統計。

要更多資料，請參閱PPPStatus homepage。

Wavemon
Wavemon是一個無線網路裝置監控軟體。

要更多資料，請參閱Wavemon網頁。

USBView
USBView顯示已連接到USB bus的裝置資料。

要更多資料，請參閱USBView網頁。

Pppconfig
Pppconfig助您自動設置ppp撥號連線。

DSL/PPPoe
DSL/PPPoe 設置PPPoE (ADSL寬頻)連線。

I810rotate
I810rotate調節 i810硬件i810switch(1)的影像輸出。

要更多資料，請參閱I810rotate網頁。

Mutt
Mutt是一個強大的文字介面MIME郵件客戶端。

要更多資料，請參閱Mutt 網頁。

Mozilla Firefox
Mozilla Firefox 瀏覽器是一個大家耳熟能詳的網站瀏覽器。

要更多資料，請參閱Mozilla Firefox 網頁。

Elinks
Elinks是一個文字介面的網站瀏覽器。

要更多資料，請參閱Elinks網頁。

34. BitDefender 救援CD 說明

這一節會教您怎樣使用BitDefender 救援CD，掃描惡意程式無論電腦上已癱瘓不能開的Windows，以至隨插即用裝置。您更可以藉本CD做更多使用手冊上沒記載的事。

34.1. 啟動BitDefender 救援光碟

要啟動光碟，從BIOS設定您的電腦由光碟機啟動，放入光碟片並啟動電腦。確認您的電腦可以由光碟機啟動。

等待螢幕畫面出現，依循著畫面的指示去進行BitDefender 救援光碟。



啟動畫面

病毒特徵碼的更新會自動進行，不需要在您每次啟動 BitDefender 救援光碟時再進行更新。

當啟動程序完成時，您將看到下一個桌面。您將開始使用BitDefender 救援CD 。



桌面

34.2. 停止BitDefender 救援光碟

在選擇離開 或執行halt指令後，您可以放心關機。



選擇 "離開"

當 BitDefender救援光碟已經成功關閉所有程式，它會顯示如以下的畫面。您可以從光碟機取出光碟片。現在可以關閉您的電腦或重新開機。

```
X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufsd) (aufsd) (aufsd) (aufsd)
ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksuspen
) (aio/0) Done.
Waiting for processes to finish.........................................
Killing processes with signal 9: (init) (aufsd) (aufsd) (aufsd) (aufsd) (
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/0
d) (khpsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.........................................
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/ini
Turning off swap... Done.
Unmounting remaining file systems.
rootfs umounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes]._
```

等待這個訊息才關機。

34.3. 如何執行一個病毒防護掃描？

開機程序完成後，一個精靈便會出現。它會提示您掃描您的電腦。您只須點擊開始按扭。



註
若您的螢幕解析度不足，系統會問您是否要用文字模式掃描。

依照三步驟指引執行掃描任務。

1. 您能見到掃描狀態和統計（掃描速度，使用時間，掃描 / 受傳染的 / 可疑的 / 隱藏的物件和其他的數目）。

   註
   掃描程序將依它的複雜程度而需花費一些時間。

2. 您可以檢視可能影響您的系統的事件數量。

   結果會以群組顯示。 點擊 "+" 的小方框以展開選項或點擊 "-" 的小方框關閉選項。

   您可以針對不同的威脅類型的分組採取行動，也可以分別進行處理。
3. 您可以檢視結果。

如果您只想掃描特定的資料夾，請選擇下列其中一個：

- 使用BitDefender Scanner for Unices。
  1. Double click the START SCANNER icon on the Desktop. This will launch the BitDefender Scanner for Unices.

2. 點擊掃描工具，將會出現一個新的視窗。
3. 選取您要掃描的資料夾並點擊開啟以使用精靈掃描。

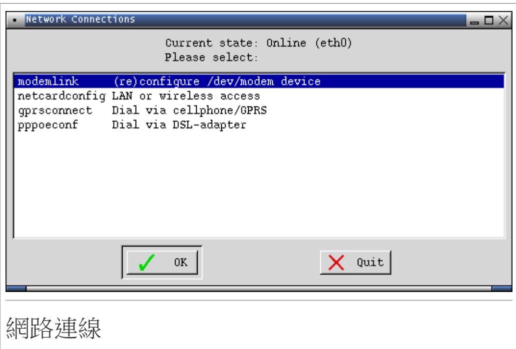
- 瀏覽您的資料夾，在檔案或目錄點擊滑鼠右鍵，選擇 傳送到。然後選擇 BitDefender 掃描器。
- 或者您可以用root執行下一個命令。BitDefender 病毒防護掃瞄開始掃描預設位置被選取的檔案或資料夾。

```
# bdscan /path/to/scan/
```

34.4. 如何設置網際網路連線？

如果您是在一個有 DHCP 的網路並且您有一塊網路卡，網際網路連線應該已經被偵測及設置。若要手動設定，請依照以下的步驟。

1. 點擊兩下桌面上的網路連線捷徑，將會出現下一個視窗。



網路連線

2. 選取您使用的連線類型並點擊確定。

連線	描述
數據機連線	當您使用數據機和電話線連線時，選取這個類型。
網路卡設置	當您使用區域網路時，選取這個類型。這同時也適用於無線網路。
GPRS連線	當您使用手機網路的GPRS (General Packet Radio Service)存取網路時，選取這個類型。
pppoe設置	如果您使用ADSL時，選取這個類型。

3. 請依照畫面的指示。如果您不確定答案，請與您的系統或網路管理者詢問。



重要
請注意您只有在選取了上述的選項之後才能啟動數據機。要設置網路連線請依照下列步驟。

1. 在桌面點擊右鍵，BitDefender救援CD 右鍵選單將會彈出。
2. 選取終端機(作為root)
3. 輸入下列指令：

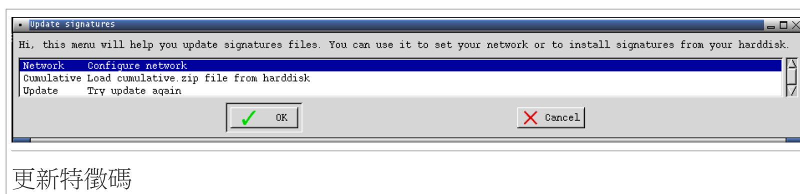
```
# pppconfig
```

4. 請依照畫面的指示。如果您不確定答案，請與您的系統或網路管理者詢問。

34.5. 如何更新BitDefender？

在開機時，將會自動更新病毒特徵碼。如果您跳過了這個步驟或想要在開機後更新，有兩個方法更新BitDefender。

- 使用BitDefender Scanner for Unices。
  1. Double click the START SCANNER icon on the desktop. This will launch the BitDefender Scanner for Unices.
  2. 點擊更新。
- 使用在桌面上的更新特徵碼捷徑。
  1. 在桌面上的更新特徵碼捷徑點擊右鍵，將會出現下一個視窗。



更新特徵碼

  2. 您可以選擇以下動作：
     - 選取累積以安裝以儲存在您的磁碟上以及透過載入cumulative.zip取得的特徵碼。。
     - 選取更新以立即連線至網際網路並取得最新的病毒特徵碼。
  3. 按下確定。

34.5.1. 如何使用proxy伺服器更新BitDefender？

若您的電腦要使用proxy伺服器才能上網，您須要做一些設定，才能更新病毒特徵碼。

要透過proxy更新BitDefender，使用下列其中一個選項：

- 使用BitDefender Scanner for Unices。

1. Double click the START SCANNER icon on the Desktop. This will launch the BitDefender Scanner for Unices.
2. 點擊設定，將會出現一個新的視窗。
3. 在更新設定，選取啟動HTTP Proxy核取方塊。 指定Proxy主機(host[:port])、Proxy用戶([domain\]username)與密碼。 點選當無可用proxy時，跳過proxy伺服器方塊，直接連線、不使用Proxy伺服器。
4. 點擊儲存。
5. 點擊更新。

● 使用Terminal (當作root)。

1. 在桌面點擊右鍵，BitDefender救援CD 右鍵選單將會彈出。
2. 選取終端機(作為root)
3. 輸入以下命令：cd /ramdisk/BitDefender-scanner/etc。
4. 輸入以下命令：mcedit bdscan.conf以GNU Midnight Commander (mc)編輯這個檔案。
5. 解除這行的註解#HttpProxy =(只是刪去#號)，再打網域，使用者名稱，密碼，伺服器連接埠。例如，這幾行一定像這樣：

   ```
   HttpProxy = myuser:mypassword@proxy.company.com:8080
   ```
6. 按下F2以儲存目前的檔案，然後點擊 F10關閉它。
7. 輸入這個命令bdscan update。

34.6. 如何儲存我的資料？

假設您因一些不知名的原因導致您不能進入Windows。同一時間，您一定得要存取一些重要的資料。這就是使用BitDefender救援CD 的時候了。

要從您的電腦取得資料並移動到卸除式磁碟，例如USB隨身碟，請依照下列步驟：

1. 將BitDefender救援CD放入光碟機，將隨身碟插入USB槽，然後重新開機。



註

如果您稍後拔出了隨身碟，您必須以照下列步驟掛載它：
a. 在桌面上的終端機模擬器捷徑點擊兩下。
b. 輸入下列命令：

```
# mount /media/sdb1
```

請注意，隨著您的電腦設置不同，它可能是sda1而不是sdb1。

2. 等到 BitDefender救援CD 完成開機。將會出現下一個視窗。



桌面

3. 點擊兩下您想復原的資料所屬的硬碟分割區(例如：[sda3]).



註

在 BitDefender救援CD 中，硬碟分割區會使用Linux-type名稱。所以[sda1]可能對應Windows-type中的(C:)，而[sda3] 對 (F:), 以及 [sdb1]指向隨身碟。



重要

如果電腦沒有正確的關機，有可能某些磁碟分割沒有自動載入。要載入磁碟分割，請依照下列步驟。

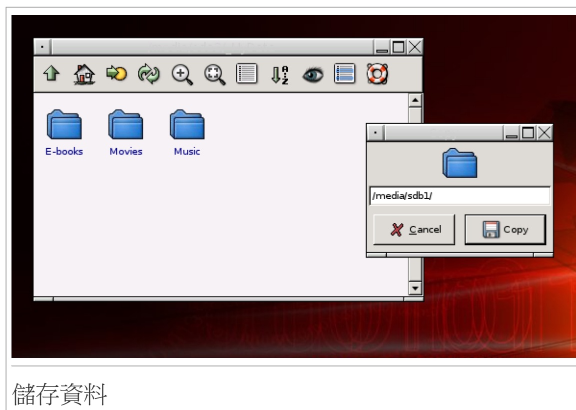
a. 在桌面上的終端機模擬器捷徑點擊兩下。

b. 輸入下列命令：

```
# mount  /media/partition_name
```

4. 瀏覽您的資料夾。例如：我的資料 包含 影片, 音樂 和 E-books子資料夾。

5. 在您想要的目錄上點擊右鍵，選取複製，將會出現下一個視窗。



儲存資料

6. 輸入/media/sdb1/至對應的欄位，然後點擊複製。

請注意，隨著您的電腦設置不同，它可能是sda1而不是sdb1。

34.7. 我該如何使用中控台模式?

If your screen resolution is not high enough to run the graphical user interface, you can run the BitDefender Rescue CD in console mode. The simple text mode allows you to perform a complete scan of your computer.

To run the CD in console mode, set up the BIOS of your computer to boot off the CD, put the CD in the drive and reboot the computer. Wait for the boot splash screen to appear and select Start knoppix in console mode.

在開機之後，依照螢幕上的指示執行一次完整的電腦掃描。

BitDefender detects the partitions on your hard drive and automatically updates the database of malware signatures before scanning begins. If any infected files are found, BitDefender will disinfect them. After the scanning process is completed, the scan log is displayed.



註

掃描程序將依它的複雜程度而需花費一些時間。

詞彙表

ActiveX

ActiveX是一個程式模型讓其他程式和作業系統執行它們。ActiveX技術是用來給微軟Internet Explorer令動態網頁比靜態網頁看起來更像電腦程式。藉由 ActiveX，使用者能使用按鈕，和其他網頁中的互動元件詢問問題或回答問題，。 ActiveX控制時常使用 Visual Basic 編寫。

ActiveX 對完全缺乏安全管控的電腦是值得注意的；電腦安全專家對它在網際網路上的ActiveX也感到沮喪。

廣告軟體

廣告軟體(Adware)通常包含在一些應用程序。這個軟件不會經使用者同意才安裝。因為這些廣告軟體在同意版權合同之後就安裝，這也是這個軟件的目的。而這個過程沒有犯罪。

然而，自動彈出(pop-up)的廣告能變成一種煩惱，同時亦會降低電腦的效率。同時，這些軟件所收集的資料可能會涉及個人私隱而安裝授權沒有完全記載。

資料封存(archive)

一個磁片 、磁帶或目錄，包含了已經備份的檔案。

檔案裡包含一個或多個以壓縮格式存在的檔案。

後門

一個系統設計者或管理員故意留下的安全漏洞，不是每個漏洞都是不好的。例如：伺服器支術員或代理商的維護電腦程式編寫員都希望要有個有特權的帳號。

開機磁區

每個硬碟的開頭都儲存了這隻硬碟的結構，(磁區大小、叢集大小等等)。若是開機硬碟，開機磁區包含着一個程序使開機時載入作業系統。

開機型病毒

一種在硬碟或磁碟上使開機磁區受感染的病毒。由磁碟開機然後蔓延至記憶體上。每次您開機，您就會啟動在記憶體的病毒。

瀏覽器

網站瀏覽器的簡稱，這個軟體用來顯示網頁。目前二大最受歡迎的瀏覽器是Netscape Navigator 及 Microsoft Internet Explorer。二者都是圖形化介面的瀏覽器，代表它們同時可以顯示圖片及文字。除此之外，在加入其他的程式元件，也可以顯示多媒體資訊，包含聲音、影片。

命令列

在命令列介面，使用者可以直接在畫面輸入命令

Cookies

在網際網路中，cookies是有關個別電腦資訊的小檔案，它又能被分析而且能被廣告界使用者追蹤您的關於上網的興趣和品味。在這範圍，cookies技術仍然繼續發展，而且意圖直接地把您感興趣的廣告瞄準著您。這是一把雙面刃。因為一方面，

這種技術會更有效率，因為您只會看到您感興趣的廣告。另一方面，事實上，它會「追蹤」並「跟隨」您去了哪和按了什麼鍵。可理解地，這有隱私上的爭論，他們覺得被網站看作"SKU數字" (就好像在包裝紙上的條碼)的辯論。當然這樣的觀點是極端的，但是在某些情況下是正確的。

磁碟機

磁碟機可允許讀取資料及寫入資料。

硬碟機可以讀取及寫入資料到硬碟。

軟碟機可以存取磁碟片。

硬碟機有包含內接式 (放置在電腦主機內) 或外接式 (放置在一個獨立的機殼裡，並與電腦主機連線)。

下載

要把資料(通常全部檔案)從一個主要的來源複製到週邊裝置。這詞語通常用來形容從線上服務到某人的電腦上。下載通常看成從網路上的檔案伺服器複製到一部電腦上。

電子郵件

電子郵件。經由本地或全球網路在電腦上傳遞郵件的服務。

事件

由軟件偵察到的一個動作或一件事件。事件可以是使用者的動作，例如：用滑鼠點擊或按鍵盤上的鍵或系統事件，例如：記憶體用完。

誤判

當掃描器識別出一個檔案受到感染，而事實上並不是。

副檔名

檔案名稱的一部份，它會跟隨在一個 "." 之後，它指出檔案是何種類型的資料。

許多作業系統使用副檔名，如：Unix、VMS 及 MS-DOS。它們通常含有一到三個字元。例如：c 代表 C 語言的原始檔、ps 則是 PostScripts 格式、txt 則是文字檔。

啟發式技術

識別新的病毒的基礎方法。這類的掃描不依賴特定的病毒驗証。好處是不會被舊病毒的變種愚弄。然而，它可能有時在正常的軟件中報告有該軟件懷疑是病毒。產生所謂的「假陽性(false positive)」。

IP

網際通訊協定－在TCP/IP中的一組通訊協定可定路線通訊協定。負責IP位址，決定路徑和IP 封包的分拆和合併。

Java applet

一個Java程序，它設計用來只是在網頁上執行。要在網頁上使用applet，您需要先定好applet的名，大小(長和闊，單位用像素)來讓applet應用。當那存取那網

頁，瀏覽器會從伺服器下載那applet，並在使用者的電腦上執行。Applet和其他的軟件分別在於Applet有嚴格的通訊協定。

例如：即使Applet在客戶端上執行，它也不能讀寫客戶端上的資料。此外，Applet在網路上有著更嚴格的監管。他們只能讀寫同一網域上的資料。

巨集型病毒

這類型的病毒是在檔案中含有巨集程式。許多應用程式如：Microsoft Word 及Excel，都有支援巨集語言。

這些應用程式允許您在一個檔案裡插入一個巨集，在檔案每一次被開啟時，巨集程式即可被執行。

電子郵件程式

一個電子郵件程式是一個應用程式，它讓您可以傳送及收發電子郵件。

記憶體

電腦內部的儲存空間。這詞語指資料被貯存為很多小碎片。而「貯存」這個詞語是指已經在磁帶或者硬碟內。每部電腦都有一定數量的實體記記憶體。通常我們通稱它為主記憶體，內存，或RAM。

非啟發式技術

這個方法是依賴特定的病毒特徵碼。非啟發式技術的好處是它不會把相似的當是病毒，以及它不會彈出錯誤的警告。

壓縮程式

一個被壓縮的格案格式。很多操作系統和應用程式包含這個命令使您把格案壓縮減少使用的記憶體。例如：您有一個文字檔案包含著十個連續的空格。通常，會用十個元組(bytes)來貯存。

然而，程式會把檔案壓縮，用一特定空格組合字元取代空白字完。在這個情況，十個空格字元會被取代成二個位元。這只是其中一隻壓縮技術，還有其他很多種。

路徑

在電腦裏到一個檔案確切的方向。 根據等級制度檔案系統，這些方向通常描述從上到下來。

兩點之間的路徑，例如：兩電腦之間的通訊頻道。

網路釣魚

將一份電子郵件送到一個使用者並，虛偽地自稱是合法的企業，並要求受害者主動地提交自己的個人資料，使犯人竊盜受害者的私人的資料。電子郵件指示使用者到一個像合法的組織的網站，更新個人的資料, 像是密碼和信用卡、社會福利和銀行帳號的網站, 。 然而，網站是假的，建立起來只是用來偷使用者的資料。

多形病毒

病毒會改變它的形式來傳染每個檔案。因為他們沒有一致的二進制樣式，這樣的病毒很難辨認。

連接埠
: 一個連接埠在您能連接設備的電腦。 個人電腦有的連接埠各種各樣的類型。 內部，有幾個口岸為連接的驅動器、顯示屏和鍵盤。 外在地，個人電腦有連接埠為連接的調制解調器、印表機、老鼠和其他外圍設備。

在TCP/IP和UDP網路，一個終點對邏輯連接。 通道數辨認什麼樣的口岸它是。 例如，連接埠80為HTTP交通使用。

報告檔案
: 這個檔案列出 BitDefender 發生的行為。BitDefender 在報告檔裡列出掃描的路徑、目錄、掃描的檔案數量及被掃描的檔案，有多少受感染及可疑檔案被發現。

Rootkit
: rootkit是一套提供系統的管理員層級存取的軟件工具。 規定為UNIX操作系統首先使用了，並且它提到了入侵者行政權利的重新編譯的工具，給他們隱存看見系統管理員。

rootkits的主要角色是掩藏過程、檔案、註冊和日誌。 如果他們合併適當的軟件，他們也許也攔截資料從終端、網路連接或者外圍設備。

Rootkits本質不是惡意的。例如，系統和有些應用使用rootkits掩藏重要檔案。然而，他們主要用於掩藏惡意程式或隱瞞入侵者已經入侵系統。 當與惡意程式結合時， rootkits造成巨大威脅和系統的安全。他們可以監測工具，建立後門系統，修改檔案和日誌和避免偵查

Script
: 有別於巨集或批次檔案，script 是一連串要被執行的命令，而且不需要使用者介入。

垃圾郵件
: 電子郵件廣告或垃圾新聞群組。通常被認為是任何未經同意的電子郵件。

間諜程式
: 存取用戶的網際網路連接隱蔽地收集用戶信息，不用他們的知識所有軟件，為做廣告通常打算。 Spyware應用典型的免費軟件或共享軟件節目一個暗藏的組分可以從網際網路被下載; 然而，值得注意的是，多數共享軟件和免費軟件應用與spyware。 一旦安裝， spyware在網際網路在背景中監測用戶活動並且傳送那信息給別人。 Spyware可能也收集關於電子郵件和密碼和甚而信用卡數字的信息。

間諜程式和木馬程式的相似之處是使用者都在安裝其他軟體時無意安裝了它們。在點對點的傳輸軟體中相當常見。

除了道德和隱私問題之外，間諜程式也占據了電腦的記憶體以及網際網路頻寬。由於間諜程式使用了您的系統資源，可能會造成您的電腦當機或系統不穩定的問題。

啟動項目
: 當電腦起動，在這個資料夾安置的所有檔案開始。 例如，一個啟動屏幕、一個酣然的檔案將運作的，當電腦首先起動時，提示日曆或者應用程序可以是起始的項目。 通常，檔案的別名在這個資料夾而不是檔案位置。

系統工具列
: 介紹與Windows 95，系統鍵盤位於視窗工作列(通常在底部的時鐘旁邊)並且包含小型圖示以簡易地存取某些系統工作，例如傳真、印表機、數據機、音量控制。點擊兩下或點擊右鍵圖式以檢視和存取細節和管控。

TCP/IP
: 傳輸控制通訊協定－一套網路通訊協定用途廣泛在提供通訊橫跨電腦在互聯的網路以不同的硬體結構和各種各樣的作業系統的網際網路。 TCP/IP包含電腦溝通標準和連接網路的協定。

木馬程式
: 一種偽裝成良性程式的破壞性程式。不同於病毒，木馬程式不複製自己，但是他們具破壞性。其中一個電腦程式內的病毒的最陰險的類型是趕走您的電腦病毒，但是又引進其他病毒。

  這個詞的來源來自荷馬史詩，希臘人送了一匹巨型木馬給他們的仇敵，特洛伊人，表面上作為和平獻禮。 但在特洛伊人將木馬拉入在他們的城市之後，希臘戰士偷偷地從木馬中爬出來並打開城門，讓他們的同胞湧入並抓住特洛伊。

更新
: 一個軟體或硬體產品的新版本，設定用來取代相同產品的舊版本。此外，更新的安裝規則需要先去檢查是否已經存在一個舊版本在您的電腦，如果不是，您無法安裝這個更新。

  BitDefender 擁有它自已的更新模組，它允許您手動檢查更新，或者讓它自動地更新軟體。

病毒
: 您的電腦没有您的了解和運作時反對被裝載某程式或一些代碼。多數病毒能也複製自己。 所有電腦人造病毒。 簡單的病毒能複製自己和相對地容易製造。 因為它將迅速使用所有可利用的記憶並且給停濟不前，這樣簡單的病毒對系統是危險的。 一個更加危險類型的病毒是一個能傳送橫跨網路和繞過保安系統。

病毒定義
: 病毒的二進位典型，被防毒軟體用來偵測並刪除病毒。

蠕蟲
: 一個在網路之上繁殖它本身的程式。它不能夠把它本身附在其他的程式。